SECURE®
COMPUTING

Secure Computing SG™
User Manual

Secure Computing
4810 Harwood Road
San Jose, CA 95124-5206
Email: support@au.securecomputing.com
Web: www.securecomputing.com

Revision 3.1.3
March 1st, 2006

Contents

1. Introduction 1

SG Gateway Appliances (SG3xx, SG5xx Series) 1

SG Rack Mount Appliances (SG7xx Series) 4

SG PCI Appliances (SG6xx Series) 7

Document Conventions 10

2. Getting Started 11

SG Gateway Appliance Quick Setup 12

SG Rack Mount Appliance Quick Setup 23

SG PCI Appliance Quick Setup 33

The SG Management Console 40

3. Network Setup 41

Configuring Connections 41

Multifunction vs. Fixed-function Ports 42

Direct Connection 44

ADSL 47

Cable Modem 52

Dialout and ISDN 53

Dialin 54

Failover, Load Balancing and High Availability 59

Internet Failover 61

Internet Load Balancing 65

High Availability 68

DMZ Network 71

Guest Network 72

Wireless 75

Bridging 86

VLANs 90

Port Based VLANs 92

GRE Tunnels 96

Routes 100

System 108

DNS 109

DHCP Server 111
Web Cache 115
QoS Traffic Shaping 123
IPv6 125
SIP 125
4. Firewall 127
Incoming Access 127
Web Server 129
Customizing the Firewall 131
Definitions 132
Packet Filtering 135
Network Address Translation (NAT) 139
Connection Tracking 151
Intrusion Detection 152
Basic Intrusion Detection and Blocking (IDB) 153
Advanced Intrusion Detection and Prevention (Snort and IPS) 156
Access Control and Content Filtering 159
Antivirus 171
5. Virtual Private Networking 182
PPTP and L2TP 183
PPTP VPN Server 183
L2TP VPN Server 191
PPTP and L2TP VPN Client 198
IPSec 200
Set Up the Branch Office 201
Configuring the Headquarters 213
Tunnel List 216
NAT Traversal Support 219
Dynamic DNS Support 219
Certificate Management 219
IPSec Failover 224
IPSec Troubleshooting 234
Port Tunnels 237

6. USB 240
USB Mass Storage Devices 240
USB Printers 247
Printer Troubleshooting 253
USB Network Devices and Modems 254
7. System 255
Date and Time 255
Backup/Restore Configuration 256
Users 259
Management 263
Diagnostics 266
Advanced 266
Reboot and Reset 269
Flash upgrade 271
Configuration Files 273
Support 274
Appendix A – Terminology 275
Appendix B – System Log 281
Access Logging 281
Creating Custom Log Rules 283
Rate Limiting 286
Administrative Access Logging 287
Boot Log Messages 287
Appendix C – Firmware Upgrade Practices and Precautions 288
Appendix D – Recovering From a Failed Upgrade 290

1. Introduction

This manual describes the features and capabilities of your SG unit, and provides you with instructions on how to best take advantage of them.

This includes setting up network connections (in the chapter entitled *Network Connections*), tailoring the firewall to your network (*Firewall*), and establishing a virtual private network (*Virtual Private Networking*). It also guides you through setting up the SG unit on your existing or new network using the web management console (*Getting Started*).

This chapter provides a high level overview to familiarize you with your SG unit's features and capabilities.

SG Gateway Appliances (SG3xx, SG5xx Series)

Note

The SG gateway appliance range includes models SG300, SG530, SG550, SG560, SG565, SG570, SG575 and SG580.

The SG gateway appliance range provides Internet security and privacy of communications for small and medium enterprises, and branch offices. It simply and securely connects your office to the Internet, and with its robust stateful firewall, shields your computers from external threats.

With the SG unit's masquerading firewall, hosts on your LAN (local area network) can see and access resources on the Internet, but all outsiders see is the SG unit's external address.

You may tailor your SG unit to disallow access from your LAN to specific Internet sites or categories of content, give priority to specific types of network traffic, and allow controlled access to your LAN from the outside world. You may also choose to enable intrusion detection and prevention services on your SG unit, to further bolster the security of your local network.

The SG565, SG560, SG570, SG575 and SG580 may also connect to a DMZ (demilitarized zone) network. A DMZ is a separate local network typically used to host servers accessible to the outside world. It is separated both physically and by the firewall, in order to shield your LAN from external traffic.

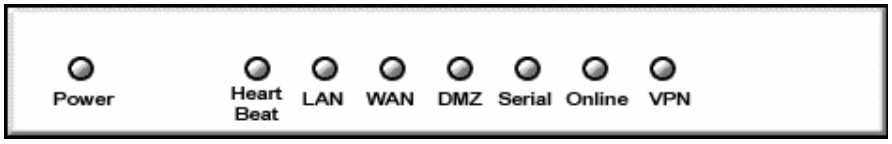
The SG unit allows you to establish a virtual private network (VPN). A VPN enables remote workers or branch offices to connect securely to your LAN over the public Internet. The SG unit can also connect to external VPNs as a client. The SG550, SG560, SG565, SG570, SG575 and SG580 utilize onboard cryptographic acceleration to ensure excellent VPN throughput.

The SG unit may be configured with multiple Internet connections. These auxiliary connections may be kept on stand-by should the primary connection become unavailable, or maintained concurrently with the primary connection for spreading network load.

The SG565, SG570, SG575 and SG580 incorporate a powerful web proxy cache to improve web page response time and reduce link loads. It is designed to integrate seamlessly with upstream proxy caches provided by ISPs.

Front panel LEDs

The front and rear panels contain LEDs indicating status. An example of the front panel LEDs are illustrated in the following figure and detailed in the following table.



Note

Not all the LEDs described below are present on all SG unit models. Labels vary from model to model.

Label	Activity	Description
Power	On	Power is supplied to the SG unit
Heart Beat	Flashing	The SG unit is operating correctly
	On	If this LED is on and not flashing, an operating error has occurred.
LAN Activity	Flashing	Network traffic on the LAN network interface

WAN Activity	Flashing	Network traffic on the Internet network interface
WLAN	Flashing	Network traffic on the Wireless network interface
DMZ Activity	Flashing	Network traffic on the DMZ network interface
Serial Activity	Flashing	For either of the SG unit COM ports, these LEDs indicate receive and transmit data
HA	On	The SG unit has switched to a backup device
Online	On	An Internet connection has been established
VPN	On	Virtual private networking is enabled
Online	On	An Internet connection has been established

Note

If Heart Beat *does not begin flashing shortly after power is supplied, refer to Appendix D,* Recovering From a Failed Upgrade.

Rear panel

The rear panel contains Ethernet and serial ports, the *Reset*/*Erase* button and power inlet. If network status LEDs are present, the lower or left LED indicates the link condition, where a cable is connected correctly to another device and the upper or right LED indicates network activity.

Specifications

Internet link

- 10/100baseT Ethernet
- Serial (for dial-up/ISDN)
- Front panel serial status LEDs (for TX/RX)
- Online status LEDs (for Internet/VPN)
- Rear panel Ethernet link and activity status LEDs

Local network link

- 10/100BaseT LAN port *(SG530, SG550)*
- 10/100BaseT 4 port LAN switch *(SG300)*
- 10/100BaseT DMZ port *(SG570, SG575)*
- 10/100BaseT 4 port VLAN-capable switch *(SG560, SG565, SG580)*
- Rear panel Ethernet link and activity status LEDs

Enviromental

- External power adaptor (voltage/current depends on individual model)
- Front panel operating status LEDs: Power, Heart Beat
- Operating temperature between 0°C and 40°C
- Storage temperature between -20°C and 70°C
- Humidity between 0 to 95% (non-condensing)

SG Rack Mount Appliances (SG7xx Series)

Note

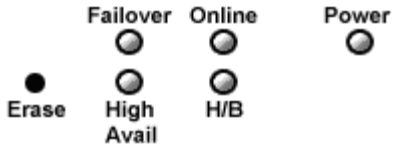
The SG rack mount appliance range includes models SG710 and SG710+.

The SG7xx series is the flagship of Secure Computing's SG family. It features multi-megabit throughput, rack-optimized form factor, two fast Ethernet ports and two 4 port fast Ethernet switches as standard, and the option for two additional gigabit ports (SG710+).

In addition to providing all of the features described in *SG Gateway Appliances* earlier in this chapter, it equips central sites to securely connect hundreds of mobile employees and branch offices.

Front panel LEDs

The front panel contains LEDs indicating status. An example of the front panel LEDs are illustrated in the following figure and detailed in the following table.



Label	Activity	Description
Power	On	Power is supplied to the SG unit
H/B (Heart Beat)	Flashing	The SG unit is operating correctly
	On	If this LED is on and not flashing, an operating error has occurred.
Failover	On	The SG unit has switched to the backup Internet connection
High Avail	On	The SG unit has switched to a backup device
Online	On	An Internet connection has been established

Note

If H/B *does not begin flashing 20 – 30 seconds after power is supplied, refer to Appendix E,* Recovering From a Failed Upgrade.

Front panel

The front panel contains two 10/100 Ethernet four port switches (*A* and *B*), two 10/100 Ethernet ports (*C* and *D*) and analog/ISDN modem (*Serial*) as well as operating status LEDs and the configuration reset button (*Erase*).

On the front panel Ethernet ports, the right hand LED indicates the *link* condition, where a cable is connected correctly to another device. The left hand LED indicates *network activity*.

Rear panel

The rear panel contains a power switch and a power inlet for an IEC power cable. Additionally, the SG710+ has two gigabit Ethernet ports (*E* and *F*).

Specifications

Internet link

- Two 10/100baseT Ethernet ports (C, D)
- Two GbE ports (E, F – *SG710+ only*)
- Serial port
- Online status LEDs (Online, Failover)
- Ethernet link and activity status LEDs

LAN/DMZ link

- Two 10/100BaseT 4 port LAN switches
- Ethernet link and activity status LEDs

Enviromental

- Front panel operating status LEDs: Power, H/B
- Operating temperature between 0°C and 40°C
- Storage temperature between -20°C and 70°C
- Humidity between 0 to 95% (non-condensing)

SG PCI Appliances (SG6xx Series)

Note

The SG PCI appliance range includes models SG630 and SG635.

The SG PCI appliance is a hardware based firewall and VPN server embedded in a 10/100 Ethernet PCI network interface card (NIC). It is installed into the host PC like a regular NIC, providing a transparent firewall to shield the host PC from malicious Internet traffic, and VPN services to allow secure remote access to the host PC.

Unlike other SG gateway and rack mount appliances, a single SG PCI appliance is not intended as a means for your entire office LAN to be connected to, and shielded from, the Internet. Installing a SG PCI appliance in each network connected PC gives it its own independently manageable, enterprise-grade VPN server and firewall, running in isolation from the host operating system.

This approach offers an increased measure of protection against internal threats as well as conventional Internet security concerns. You can update, configure and monitor the firewall and VPN connectivity of a workstation or server from any web browser. In the event of a breach, you have complete control over access to the host PC independent of its operating system, even if the host PC has been subverted and is denying normal administrator access.

All network filtering and CPU intensive cryptographic processing is handled entirely by the SG unit. This has the advantage over the traditional approach of using a host-based personal software firewall and VPN service by not taxing the host PC's resources.

Bridged mode

By default, the SG PCI appliance operates in bridged mode. This is distinctly different from the masquerading behavior of SG gateway and rack mount appliances.

In bridged mode, the SG PCI appliance uses two IP addresses. Note that these addresses are both in the same subnet as the LAN, as no masquerading is being performed (refer to the *Masquerading* section of the chapter entitled *Firewall* for further details).

One IP address is used to manage the SG unit via the web management console.

The other is the host PC's IP address, which is configurable through the host operating system, identically to a regular NIC. This is the IP address that other PCs on the LAN see. It should be dynamically (DHCP) or statically configured to use the same gateway, DNS, etc. settings as a regular PC on the LAN.

Note

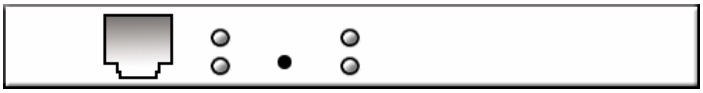
It is possible to configure the SG PCI appliance to run in masquerading mode. This is discussed in the chapter entitled Firewall*.*

Secure by default

By default, all SG units run a fully secured stateful firewall. This means from the PC that it is plugged into, most network resources are freely accessible. However, any services that the PC provides, such as file shares or web services (e.g. IIS) are *not* be accessible by other hosts on your LAN without further configuration of the SG unit. This is accomplished using packet filter rules, for details refer to the *Packet Filtering* section of the chapter entitled *Firewall*.

LEDs

The rear panel contains LEDs indicating status. The two LEDs closest to the network port are network activity (upper) and network link (lower). The two other LEDs are power (upper) and heart beat (lower).



Location	Activity	Description
Top right (*Power*)	On	Power is supplied to the SG unit (top right).
Bottom right (*Heart beat*)	Flashing	The SG unit is operating correctly (bottom right).
Top left (*Network activity*)	Flashing	Data is being transmitted or received (top left).
Bottom left (*Network link*)	On	The SG unit is attached to the network

Note

If Heart beat *does not begin flashing shortly after power is supplied, refer to Appendix D,* Recovering From a Failed Upgrade.

Specifications

Network link

- 10/100baseT Ethernet port
- Ethernet LEDs (link, activity)

Environmental

- Status LEDs: Power, Heart Beat
- Operating temperature between 0°C and 40°C
- Storage temperature between -20°C and 70°C
- Humidity between 0 to 95% (non-condensing)

Document Conventions

This document uses different fonts and typefaces to show specific actions.

Warning/Note

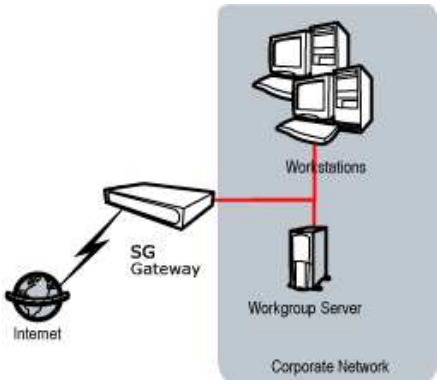
Text like this highlights important issues.

Bold text in procedures indicates text that you type, or the name of a screen object (e.g. a menu or button).

2. Getting Started

This chapter provides step-by-step instructions for installing your SG unit. These instructions are identical to those in the printed *Quick Install Guide* that shipped with your SG unit.

Upon completing the steps in this chapter, your SG gateway or rack mount appliance is installed in a network configuration similar that depicted in the figure to the right. If you are setting up a SG PCI appliance, upon completing the steps in this chapter, your host PC is connected securely to your existing LAN.



These instructions assume you have a PC running Microsoft Windows (95/98/Me/2000/XP for SG gateway and rack mount appliances, 2000/XP only for SG PCI appliances). If you are installing a SG gateway or rack mount appliance, you must have an Ethernet network interface card installed. You may need to be logged in with administrator privileges.

Instructions are not given for other operating systems; refer to your operating system documentation on how to configure your PCs' network settings using the examples given for Windows PCs as a guide.

Note

Installing your SG unit into a well-planned network is easy. However, network planning is outside the scope of this manual. Please take the time to plan your network before installing your SG unit.

- If you are setting up a SG gateway appliance (SG3xx, SG5xx series) proceed to *SG Gateway Appliance Quick Setup*.
- If you are setting up a SG rack mount appliance (SG7xx series) proceed to *SG Rack Mount Appliance Quick Setup*.
- If you are setting up a SG PCI appliance (SG6xx series), proceed to *SG PCI Appliance Quick Setup*.

SG Gateway Appliance Quick Setup

Unpack the SG unit

Check that the following items are included with your SG unit:

- Power adapter
- SG CD
- Network cable

On the rear panel of the SG unit you will see network, serial and possibly USB ports, a **Reset**/**Erase** button, and a power inlet.

The front panel of the SG unit contains activity LEDs (lights) that vary slightly between models. These provide information on the operating status of the SG unit.

Note

Power is ON when power is applied (use only the power adapter packaged with the unit).

***System**/**Heart Beat**/**TST** flashes when the SG unit is running.*

*Initially, all appliance models except for the **SG300** also have all other front panel LEDs flashing.*

*If these LEDs do not behave in this manner before your SG unit is attached to the network, perform a factory reset. Press the black **Reset**/**Erase** button on rear panel **twice** within two seconds to restore factory default settings. If the LEDs are still not flashing after 30 seconds, you may need to contact customer support.*

Set up a single PC to connect to the SG unit

The SG unit ships with initial network settings of:

LAN IP address: **192.168.0.1**

LAN subnet mask: **255.255.255.0**

The SG unit needs an IP address suitable for your LAN before it is connected. You may choose to use the SG unit's initial network settings above as a basis for your LAN settings.

Connect the supplied power adapter to the SG unit.

- ◇ If you are setting up the **SG300**, attach your PC's network interface card directly to any network port on its **LAN** switch using the supplied network cable.
- ◇ If you are setting up the **SG560**, **SG565** or **SG580**, attach your PC's network interface card directly any network port on switch **A** (**A1** – **A4**) using the supplied network cable.
- ◇ Otherwise, connect the SG unit's **LAN** network port directly to your PC's network interface card using the supplied network cable.

Note

At this point, if you attach the SG unit directly to a LAN with an existing DHCP server, or a PC running a DHCP service, it will automatically obtain an additional address. The SG unit will still be reachable at 192.168.0.1.

However, we strongly recommend that you do not connect the SG unit to your LAN until instructed to do so by this guide.

All other network ports are by default inactive, i.e. they are not running any network services such as DHCP, and they are not configured with an IP address.

Next, modify your PC's network settings to enable it to communicate with the SG unit.

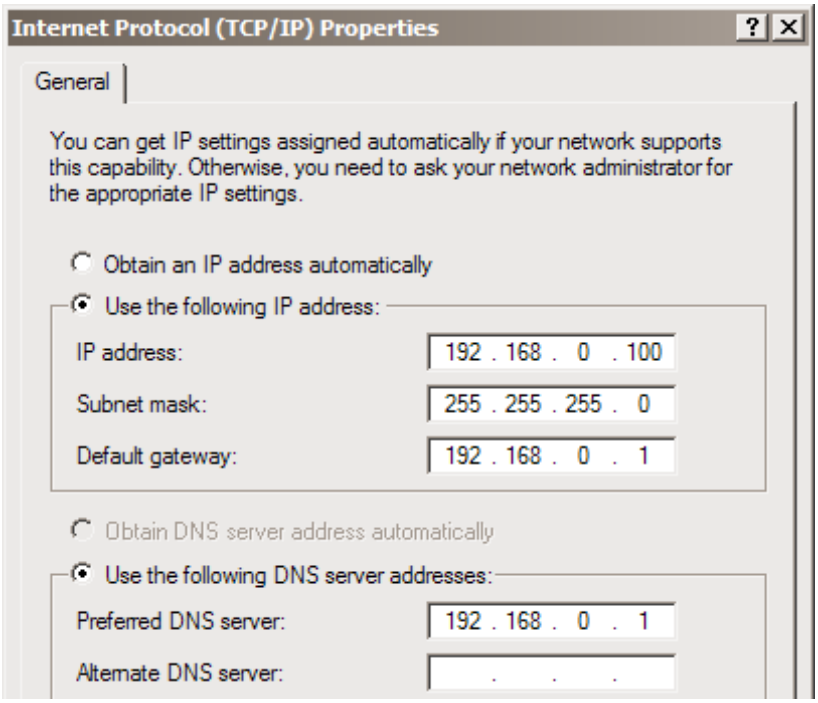
Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections** (or in 95/98/Me, double click **Network**).

Right click on **Local Area Connection** and select **Properties**.

Note

If there is more than one existing network connection, select the one corresponding to the network interface card to which the SG unit is attached.

Select **Internet Protocol (TCP/IP)** and click **Properties** (or in 95/98/Me, **TCP/IP** -> ***your network card name*** if there are multiple entries) and click **Properties**.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 100
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
192 . 168 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
192 . 168 . 0 . 1
Alternate DNS server:

Select **Use the following IP address** and enter the following details:

IP address:	**192.168.0.100**
Subnet mask:	**255.255.255.0**
Default gateway:	**192.168.0.1**

Select **Use the following DNS server addresses** and enter:

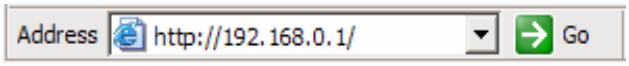
Preferred DNS server:	**192.168.0.1**

Note

If you wish to retain your existing IP settings for this network connection, click Advanced and Add the secondary IP address of 192.168.0.100, subnet mask 255.255.255.0.

Set up the SG unit's password and LAN connection settings

Launch your web browser and navigate to **192.168.0.1**.



Select **Quick Setup Wizard** from the center of the page.

A log in prompt is displayed. Enter the initial user name and password for the SG unit:

User name: **root**

Password: **default**

Note

If you are unable to browse to the SG unit at 192.168.0.1, or the initial username and password are not accepted, press the black Reset/Erase button on the SG unit's rear panel twice, wait 20 – 30 seconds, then try again.

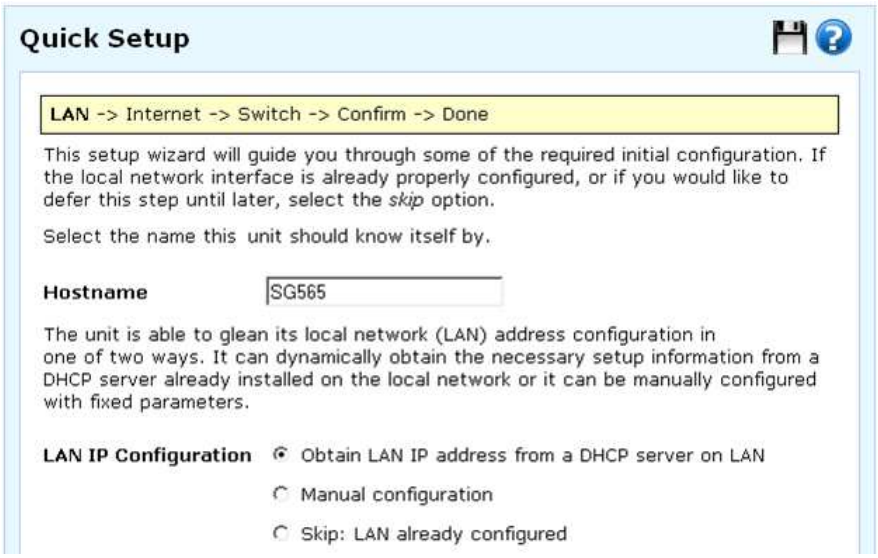
Pressing Reset/Erase twice within 2 seconds resets the SG unit to its factory default settings.

Enter and confirm a password for your SG unit. This is the password for the user **root**, the main administrative user account on the SG unit. It is therefore important that you choose a password that is hard to guess, and keep it safe.

Note

The new password takes effect immediately. You are prompted to enter it when completing the next step.

The quick setup wizard is displayed.


Quick Setup
LAN -> Internet -> Switch -> Confirm -> Done
This setup wizard will guide you through some of the required initial configuration. If the local network interface is already properly configured, or if you would like to defer this step until later, select the skip option.
Select the name this unit should know itself by.
Hostname
SG565
The unit is able to glean its local network (LAN) address configuration in one of two ways. It can dynamically obtain the necessary setup information from a DHCP server already installed on the local network or it can be manually configured with fixed parameters.
LAN IP Configuration
Obtain LAN IP address from a DHCP server on LAN
Manual configuration
Skip: LAN already configured

Changing the **Hostname** is not typically necessary.

Select how you would like to set up your LAN connection then click **Next**.

Note

*You must select **Manual configuration** in order to enable the SG unit's built-in DHCP server. The SG unit's DHCP server automatically configures the network settings of PCs and other hosts on your LAN.*

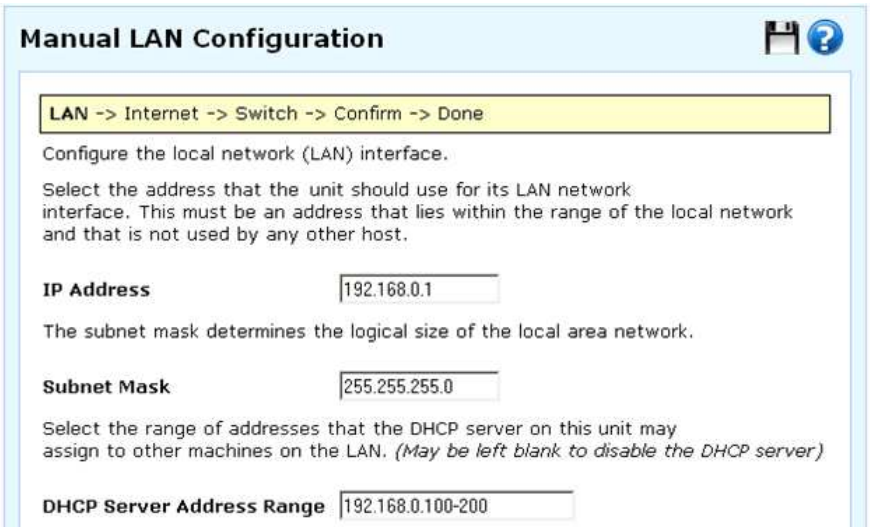
Changes to the SG unit's LAN configuration do not take effect until the quick setup wizard has completed.

◇ Select **Manual configuration** to manually specify the SG unit's LAN connection settings *(recommended)*.

◇ Select **Skip: LAN already configured** if you wish to use the SG unit's initial network settings (IP address **192.168.0.1** and subnet mask **255.255.255.0**) as a basis for your LAN settings, and you do not wish to use the SG unit's built-in DHCP server. Skip to the next step.

◇ You may choose to **Obtain LAN IP address from a DHCP server on LAN** if you have an existing DHCP server, and wish to rely on it to automatically configure the SG unit's LAN connection settings *(not recommended)*. Skip to the next step.

If you selected **Manual configuration**, some additional information is required. Otherwise, skip to the next step.


Manual LAN Configuration
LAN -> Internet -> Switch -> Confirm -> Done
Configure the local network (LAN) interface.
Select the address that the unit should use for its LAN network interface. This must be an address that lies within the range of the local network and that is not used by any other host.
IP Address
192.168.0.1
The subnet mask determines the logical size of the local area network.
Subnet Mask
255.255.255.0
Select the range of addresses that the DHCP server on this unit may assign to other machines on the LAN. (May be left blank to disable the DHCP server)
DHCP Server Address Range
192.168.0.100-200

Enter an **IP address** and **Subnet Mask** for the SG unit's LAN connection.

Note

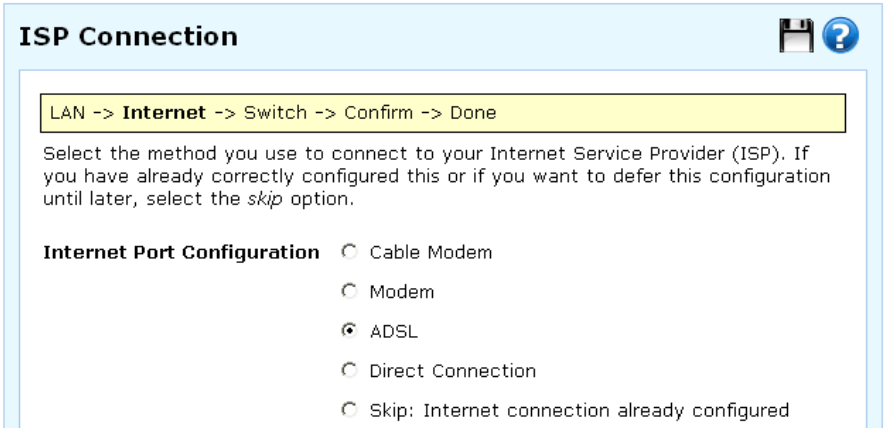
Take note of this IP address and subnet mask, as you will need them later on.

To enable the SG unit's built-in DHCP server, enter a range of addresses to hand out in **DHCP Server Address Range**. PCs and other hosts on your LAN that are set to automatically obtain network settings are assigned an address from this range, and instructed to use the SG unit as their gateway to the Internet and as their DNS server for Internet domain name resolution.

Click **Next**.

Set up the SG unit's Internet connection settings

First, attach the SG unit to your modem device or Internet connection medium. If necessary, give the modem device some time to power up.


ISP Connection
LAN -> Internet -> Switch -> Confirm -> Done
Select the method you use to connect to your Internet Service Provider (ISP). If you have already correctly configured this or if you want to defer this configuration until later, select the skip option.
Internet Port Configuration
Cable Modem
Modem
ADSL
Direct Connection
Skip: Internet connection already configured

Select your Internet connection type and click **Next**. The options displayed differ depending on the connection type selected.

- If you are connecting using a **Cable Modem**, select your ISP, or **Generic Cable Modem Provider** if yours does not appear.
- If you are connecting using an analog (dialup) **Modem**, enter the details provided by your ISP.
- If you are connecting using an **ADSL** modem, select **Auto detect ADSL connection type**, click **Next**, then enter the details provided by your ISP. If auto detection fails, you must manually select your ADSL connection type – if you are unsure of this, contact your ISP.
- If you have a **Direct Connection** to the Internet (e.g. a leased line), enter the IP settings provided by your ISP.

Note

*For detailed help for each of these options, please refer to the user manual on the SG CD (**\doc\UserManual.pdf**).*

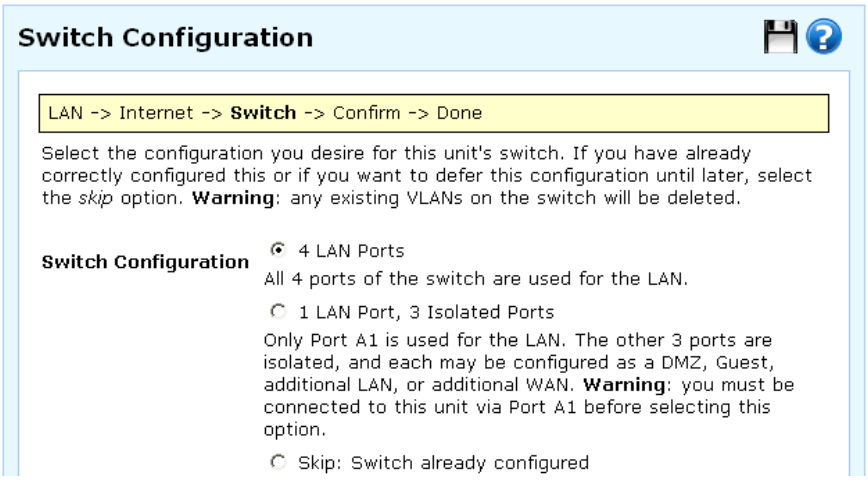
After entering the appropriate details, click **Next**.

Set up the SG unit's switch

Note

*This page will only display if you are setting up the **SG560**, **SG565** or **SG580**. Otherwise skip to the next step.*

By default, the SG unit's switch **A** behaves as a conventional switching hub. However, it may be configured so that each port behaves as if it were physically separate from the others.


Switch Configuration
LAN -> Internet -> Switch -> Confirm -> Done
Select the configuration you desire for this unit's switch. If you have already correctly configured this or if you want to defer this configuration until later, select the skip option. Warning: any existing VLANs on the switch will be deleted.
Switch Configuration
4 LAN Ports
All 4 ports of the switch are used for the LAN.
1 LAN Port, 3 Isolated Ports
Only Port A1 is used for the LAN. The other 3 ports are isolated, and each may be configured as a DMZ, Guest, additional LAN, or additional WAN. Warning: you must be connected to this unit via Port A1 before selecting this option.
Skip: Switch already configured

Select a configuration for the SG unit's switch then click **Next**.

◇ Select **1 LAN Port, 3 Isolated Ports** if you require multiple network segments, such as a DMZ, guest network or second LAN, or if you want to use multiple broadband Internet connections for Internet load balancing or Internet failover. Port **A1** is used as the primary LAN connection.

Note

For instructions on setting up multiple network segments and Internet connections, please refer to the next chapter of this manual.

◇ Otherwise, select **4 LAN Ports**.

Connect the SG unit to your LAN

Review your configuration changes. Once you are satisfied, click **Finish** to activate the new configuration.

Note

If you have changed the SG unit's LAN connection settings, it may become uncontactable at this point. This step describes how to set up the PCs on your network to access the SG unit and the Internet.

Connect the SG unit to your LAN if you haven't already done so.

- ◇ If you are setting up the **SG300**, connect PCs and/or your LAN hub directly to its **LAN** switch.
- ◇ If you are setting up the **SG560**, **SG565** or **SG580** and have configured its switch as **4 LAN Ports**, connect PCs and/or your LAN hub directly to switch **A**.
- ◇ If you are setting up the **SG560**, **SG565** or **SG580** and have configured its switch as **1 LAN Port, 3 Isolated Ports**, connect port **A1** directly to your LAN hub.
- ◇ Otherwise, connect the **LAN** port directly to your LAN hub.

Set up your LAN to access the Internet

To access the Internet, each PC on your LAN must be assigned an appropriate IP address, and have the SG unit's LAN IP address designated as its gateway and as its DNS server.

A DHCP server allows PCs to automatically obtain these network settings when they start up. If your network does not have a DHCP server, you may either manually set up each PC on your network, or set up the SG unit's DHCP server.

- ◇ To use the SG unit's built-in DHCP server *(recommended)*, proceed to *Automatic configuration of your LAN.*
- ◇ If your LAN already has a DHCP server that you will use instead of the SG unit's built-in DHCP server, proceed to *Automatic configuration of your LAN using an existing DHCP server*.

◇ If you do not want to use a DHCP server, proceed to *Manual configuration of your LAN*.

Automatic configuration of your LAN

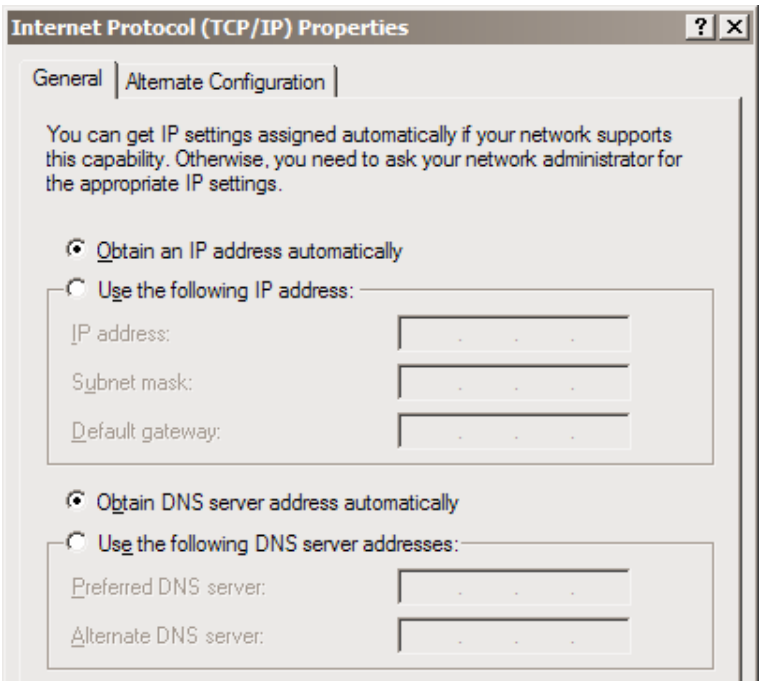
By selecting **Manual Configuration** for the SG unit's LAN connection, and supplying **DHCP Server Address Range**, the SG unit's DHCP server is already set up and running.

Each PC on your LAN must now be set up to automatically obtain network settings.

Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections** (or in 95/98/Me, double click **Network**).

If presented with multiple connections, right click on **Local Area Connection** (or appropriate network connection) and select **Properties**.

Select **Internet Protocol (TCP/IP)** and click **Properties** (or in 95/98/Me, **TCP/IP -> [your network card name]** if there are multiple entries) and click **Properties** (in 95/98/Me, you may also have to click the **IP Address** tab).


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

Check **Obtain an IP address automatically**, check **Obtain DNS server address automatically** and click **OK** (in 95/98/Me, reboot the PC if prompted to do so).

Quick setup is now complete.

Automatic configuration of your LAN using an existing DHCP server

- ◇ If you chose to have the SG unit **Obtain LAN IP address from a DHCP server on LAN**, It is strongly recommended that you add a lease to your existing DHCP server to reserve the IP address you chose for the SG unit's LAN connection.
- ◇ If you chose to set the SG unit's LAN connection settings using **Manual configuration**, you may simply remove this address from the pool of available addresses.

Enter this same IP address as the *gateway IP address* to be handed out by the existing DHCP server.

Enter this same IP address as the *DNS server IP address* to be handed out by the DHCP server.

Ensure all PCs on the network are set up to automatically obtain network configuration as per *Automatic configuration of your LAN*, then restart them.

Note

The purpose of restarting the computers is to force them to update their automatically configured network settings. Alternatively you can use a utility such as ipconfig to release then renew the DHCP lease, or disable and re-enable the network connection.

Quick setup is now complete.

Manual configuration of your LAN

Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections** (or in 95/98/Me, double click **Network**).

If presented with multiple connections, right click on **Local Area Connection** (or appropriate network connection) and select **Properties**.

Select **Internet Protocol (TCP/IP)** and click **Properties** (or in 95/98/Me, **TCP/IP -> [your network card name]** if there are multiple entries).

Enter the following details:

- **IP address** is an IP address that is part of the same subnet range as the SG unit's LAN connection (if using the default settings, 192.168.0.2 – 192.168.0.254).
- **Subnet mask** is the subnet mask of the SG unit's LAN connection (if using the default settings, 255.255.255.0).
- **Default gateway** is the IP address of the SG unit's LAN connection (if using the default settings, 192.168.0.1).
- **Preferred DNS server** is the IP address of the SG unit's LAN connection (if using the default settings, 192.168.0.1).

Click **OK** (or in 95/98/Me, **Add** then **OK**, reboot the PC if prompted to do so).

Perform these steps for each PC on your network.

Quick setup is now complete.

SG Rack Mount Appliance Quick Setup

Unpack the SG unit

Check that the following items are included with your SG unit:

- Power cable
- SG CD
- Network cable

The front panel of the SG unit has two 4- port network switches (**A** and **B**), two network ports (**C** and **D**), a serial port, status LEDs and **Erase** button.

The rear panel of the SG unit has a power inlet and power switch.

Note

Additionally, the SG710+ has two gigabit network ports on the rear panel (E and F).

The status LEDs on the front panel provide information on the operating status of the SG unit.

Note

Power is ON when power is applied. H/B (heart beat) flashes when the SG unit is running. Each of the network ports has two LEDs indicating link, activity and speed. In its factory default state, the four status LEDs next to Power flash.

If these LEDs do not behave in this manner *before* your SG unit is attached to the network, perform a factory reset. Press the black **Erase** button on front panel **twice** within two seconds to restore factory default settings. If the LEDs are still not flashing after 30 seconds, you may need to contact customer support.

Set up a single PC to connect to the SG unit

The SG unit ships with initial network settings of:

LAN IP address: **192.168.0.1**

LAN subnet mask: **255.255.255.0**

The SG unit needs an IP address suitable for your LAN before it is connected. You may choose to use the SG unit's initial network settings above as a basis for your LAN settings.

Note

Initial configuration is performed through a port on network switch A (A1 – A4). If you attach A1 – A4 directly to a LAN with an existing DHCP server, or a PC running a DHCP service, it will automatically obtain an additional address. The SG unit will still be reachable at 192.168.0.1.

However, we strongly recommend that you do not connect the SG unit to your LAN until instructed to do so by this guide.

All other network ports are by default inactive, i.e. they are not running any network services such as DHCP, and they are not configured with an IP address.

Connect the supplied power cable to the power inlet on the rear panel of the SG unit and turn on the rear panel power switch.

Connect one of the ports of network switch **A** (**A1** – **A4**) directly to your PC's network interface card using the supplied network cable.

Next, modify your PC's network settings to enable it to communicate with the SG unit.

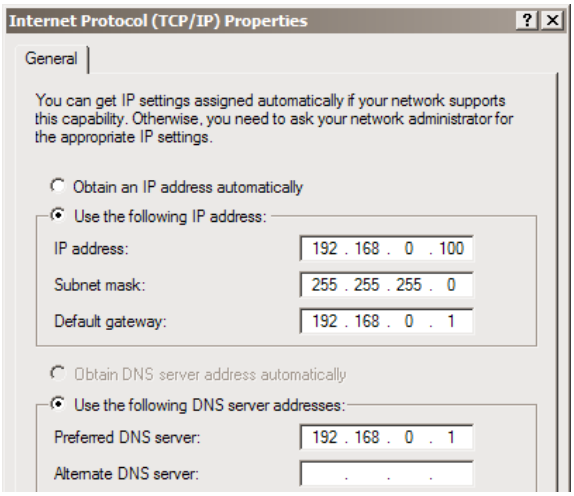
Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections** (or in 95/98/Me, double click **Network**).

Right click on **Local Area Connection** and select **Properties**.

Note

If there is more than one existing network connection, select the one corresponding to the network interface card to which the SG unit is attached.

Select **Internet Protocol (TCP/IP)** and click **Properties** (or in 95/98/Me, **TCP/IP** -> ***your network card name*** if there are multiple entries) and click **Properties**.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server:

Select **Use the following IP address** and enter the following details:

IP address:	**192.168.0.100**
Subnet mask:	**255.255.255.0**
Default gateway:	**192.168.0.1**

Select **Use the following DNS server addresses** and enter:

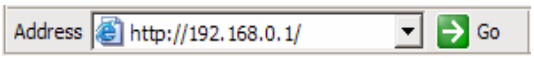
Preferred DNS server: **192.168.0.1**

Note

If you wish to retain your existing IP settings for this network connection, click Advanced and Add the secondary IP address of 192.168.0.100, subnet mask 255.255.255.0.

Set up the SG unit's password and LAN connection settings

Launch your web browser and navigate to **192.168.0.1**.



Select **Quick Setup Wizard** from the center of the page.

A log in prompt is displayed. Enter the initial user name and password for the SG unit:

User name: **root**

Password: **default**

Note

If you are unable to browse to the SG unit at 192.168.0.1, or the initial username and password are not accepted, press the black Erase button on the SG unit's front panel twice, wait 20 – 30 seconds, then try again.

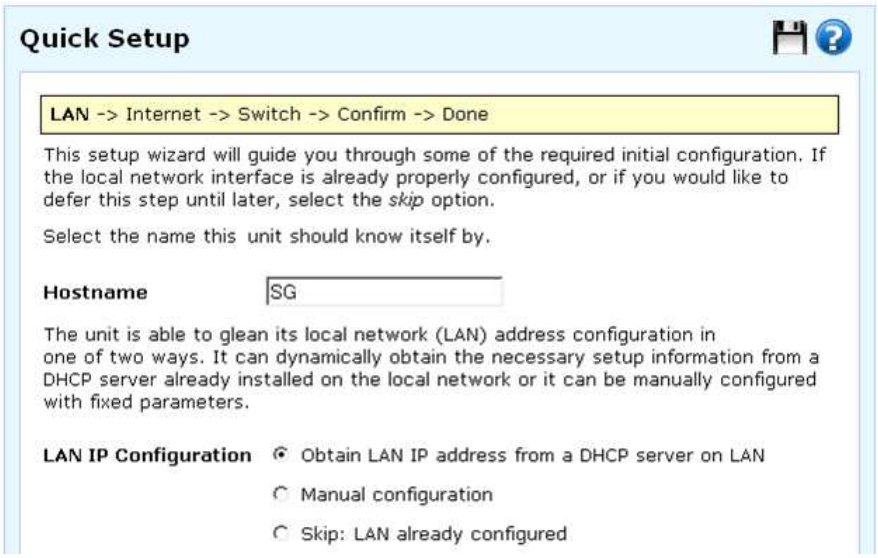
*Pressing **Erase** twice within 2 seconds resets the SG unit to its factory default settings.*

Enter and confirm a password for your SG unit. This is the password for the user **root**, the main administrative user account on the SG unit. It is therefore important that you choose a password that is hard to guess, and keep it safe.

Note

The new password takes effect immediately. You are prompted to enter it when completing the next step.

The quick setup wizard is displayed.


Quick Setup
LAN -> Internet -> Switch -> Confirm -> Done
This setup wizard will guide you through some of the required initial configuration. If the local network interface is already properly configured, or if you would like to defer this step until later, select the skip option.
Select the name this unit should know itself by.
Hostname
SG
The unit is able to glean its local network (LAN) address configuration in one of two ways. It can dynamically obtain the necessary setup information from a DHCP server already installed on the local network or it can be manually configured with fixed parameters.
LAN IP Configuration
Obtain LAN IP address from a DHCP server on LAN
Manual configuration
Skip: LAN already configured

Changing the **Hostname** is not typically necessary.

Select how you would like to set up your LAN connection then click **Next**.

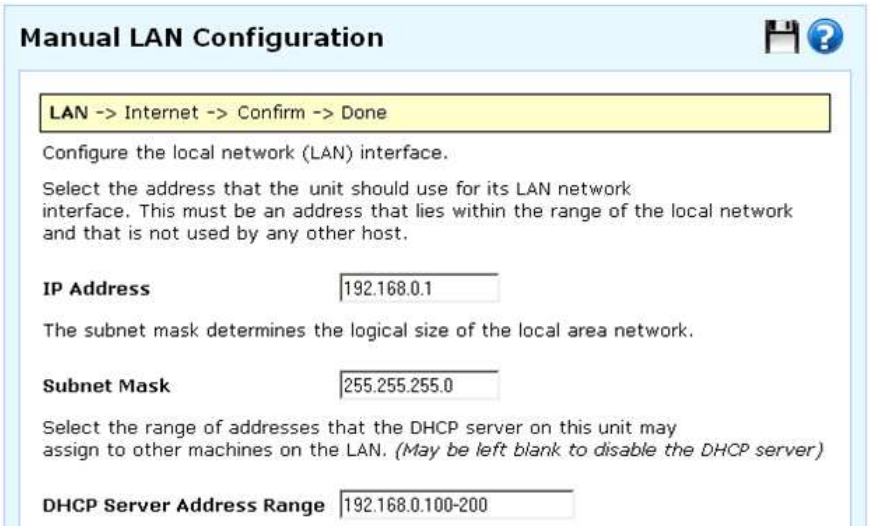
Note: You must select **Manual configuration** in order to enable the SG unit's built-in DHCP server. The SG unit's DHCP server automatically configures the network settings of PCs and other hosts on your LAN.

Changes to the SG unit's LAN configuration do not take effect until the quick setup wizard has completed.

- ◇ Select **Manual configuration** to manually specify the SG unit's LAN connection settings *(recommended)*.
- ◇ Select **Skip: LAN already configured** if you wish to use the SG unit's initial network settings (IP address **192.168.0.1** and subnet mask **255.255.255.0**) as a basis for your LAN settings, and you do not wish to use the SG unit's built-in DHCP server. Skip to the next step.

◇ You may choose to **Obtain LAN IP address from a DHCP server on LAN** if you have an existing DHCP server, and wish to rely on it to automatically configure the SG unit's LAN connection settings *(not recommended)*. Skip to the next step.

If you selected **Manual configuration**, some additional information is required. Otherwise, skip to the next step.


Manual LAN Configuration
LAN -> Internet -> Confirm -> Done
Configure the local network (LAN) interface.
Select the address that the unit should use for its LAN network interface. This must be an address that lies within the range of the local network and that is not used by any other host.
IP Address
192.168.0.1
The subnet mask determines the logical size of the local area network.
Subnet Mask
255.255.255.0
Select the range of addresses that the DHCP server on this unit may assign to other machines on the LAN. (May be left blank to disable the DHCP server)
DHCP Server Address Range
192.168.0.100-200

Enter an **IP address** and **Subnet Mask** for the SG unit's LAN connection.

Note

Take note of this IP address and subnet mask, as you will need them later on.

To enable the SG unit's built-in DHCP server, enter a range of addresses to hand out in **DHCP Server Address Range**. PCs and other hosts on your LAN that are set to automatically obtain network settings are assigned an address from this range, and instructed to use the SG unit as their gateway to the Internet and as their DNS server for Internet domain name resolution.

Click **Next**.

Connect the SG unit to your LAN

Review your configuration changes. Once you are satisfied, click **Finish** to activate the new configuration.

Note

If you have changed the SG unit's LAN connection settings, it may become uncontactable at this point. This step describes how to set up the PCs on your network to access the SG unit and the Internet.

Connect PCs and/or your LAN hub to switch **A** on the SG unit.

Set up the PCs on your LAN

Each PC on your LAN must now be assigned an appropriate IP address, and have the SG unit's LAN IP address designated as its gateway and as its DNS server.

A DHCP server allows PCs to automatically obtain these network settings when they start up. If your network does not have a DHCP server, you may either manually set up each PC on your network, or set up the SG unit's DHCP server.

- ◇ To use the SG unit's built-in DHCP server *(recommended)*, proceed to *Automatic configuration of your LAN*.
- ◇ If your LAN already has a DHCP server that you will use instead of the SG unit's built-in DHCP server, proceed to *Automatic configuration of your LAN using an existing DHCP server*.
- ◇ If you do not want to use a DHCP server, proceed to *Manual configuration of your LAN*.

Automatic configuration of your LAN

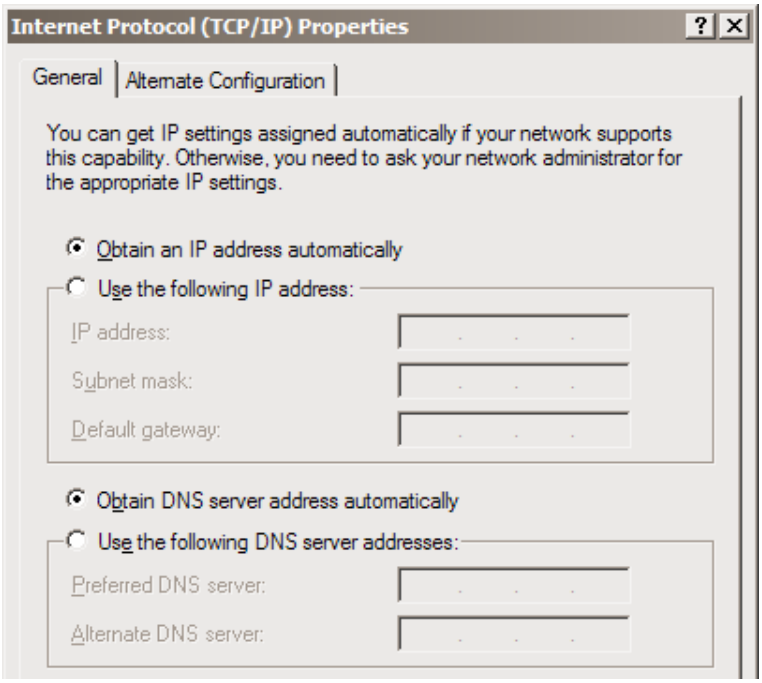
By selecting **Manual Configuration** for the SG unit's LAN connection, and supplying **DHCP Server Address Range**, the SG unit's DHCP server is already set up and running.

Each PC on your LAN must now be set up to automatically obtain network settings.

Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections** (or in 95/98/Me, double click **Network**).

If presented with multiple connections, right click on **Local Area Connection** (or appropriate network connection) and select **Properties**.

Select **Internet Protocol (TCP/IP)** and click **Properties** (or in 95/98/Me, **TCP/IP -> [your network card name]** if there are multiple entries) and click **Properties** (in 95/98/Me, you may also have to click the **IP Address** tab).


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

Check **Obtain an IP address automatically**, check **Obtain DNS server address automatically** and click **OK** (in 95/98/Me, reboot the PC if prompted to do so).

Automatic configuration of your LAN using an existing DHCP server

- If you chose to have the SG unit **Obtain LAN IP address from a DHCP server on LAN**, It is strongly recommended that you add a lease to your existing DHCP server to reserve the IP address you chose for the SG unit's LAN connection.
- If you chose to set the SG unit's LAN connection settings using **Manual configuration**, you may simply remove this address from the pool of available addresses.

Enter this same IP address as the *gateway IP address* to be handed out by the existing DHCP server.

Enter this same IP address as the *DNS server IP address* to be handed out by the DHCP server.

Ensure all PCs on the network are set up to automatically obtain network configuration as per *Automatic configuration of your LAN*, then restart them.

Note

The purpose of restarting the computers is to force them to update their automatically configured network settings. Alternatively you can use a utility such as ipconfig to release then renew the DHCP lease, or disable and re-enable the network connection.

Manual configuration of your LAN

Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections** (or in 95/98/Me, double click **Network**).

If presented with multiple connections, right click on **Local Area Connection** (or appropriate network connection) and select **Properties**.

Select **Internet Protocol (TCP/IP)** and click **Properties** (or in 95/98/Me, **TCP/IP -> [your network card name]** if there are multiple entries).

Enter the following details:

- **IP address** is an IP address that is part of the same subnet range as the SG unit's LAN connection (e.g. if using the default settings, 192.168.0.2 – 192.168.0.254).
- **Subnet mask** is the subnet mask of the SG unit's LAN connection (if using the default settings, 255.255.255.0).
- **Default gateway** is the IP address of the SG unit's LAN connection (if using the default settings, 192.168.0.1).
- **Preferred DNS server** is the IP address of the SG unit's LAN connection (if using the default settings, 192.168.0.1).

Click **OK** (or in 95/98/Me, **Add** then **OK**, reboot the PC if prompted to do so).

Perform these steps for each PC on your network.

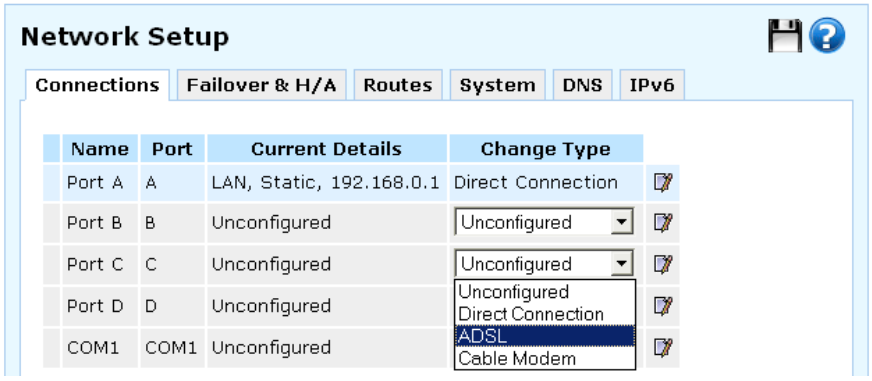
Set up the SG unit's Internet connection settings

Choose a port on the SG unit for your primary Internet connection. **Port C** is used in this guide. Attach **Port C** to your modem device or Internet connection medium. If necessary, give the modem device some time to power up.

Note

If you have changed the SG unit's LAN connection settings, browse to the new LAN IP address.

Select **Network Setup** from the **Network Setup** menu.



In the row labeled **Port C**, select your Internet connection type from the **Change Type** drop down list.

- ◇ If you are connecting using a **Cable Modem**, select your ISP, or **Generic Cable Modem Provider** if yours does not appear.
- ◇ If you are connecting using an **ADSL** modem, select **Auto detect ADSL connection type**, click **Next**, then enter the details provided by your ISP. If auto detection fails, you must manually select your ADSL connection type – if you are unsure of this, contact your ISP.
- ◇ If you have a **Direct Connection** to the Internet (e.g. a leased line), enter the IP settings provided by your ISP.

Note

For detailed help for each of these options, please refer to the next chapter.

After entering the appropriate details, click **Finish**.

Quick setup is now complete.

SG PCI Appliance Quick Setup

Unpack the SG unit

Check that the SG CD is included with your appliance:

On the SG unit is a single 10/100 network port, a **Reset** button and four LEDs (lights). The LEDs provide information on the operating status of your SG unit. The two LEDs closest to the network port indicate **network link** and **network activity**.

The two LEDs furthest from the network port indicate **Power** and **Heart Beat**. The Heart Beat LED blinks when the SG unit is running. The Power LED is ON when power is applied.

Install the SG unit in an unused PCI slot

Power off your PC and remove its cover.

Select an unused PCI slot and insert the SG unit.

Power on your PC.

Install the network driver on your PC

The SG unit is automatically detected and the appropriate driver is installed when Windows starts up. It is detected as a Realtek RTL8139-series Fast Ethernet Adapter.

Note

*You can check that a new network adapter has been installed by clicking **Start** -> (**Settings** ->) **Network and Dialup Connections** -> **Local Area Connection** (possibly followed by a number) -> **Properties** and ensure the adapter is listed in the **Connect using** field.*

Set up your PC to connect to the web management console

Note

The following steps assume you want to set up your SG unit in bridged mode, so that it sits between your PC and the LAN, transparently filtering network traffic.

If you want to set up your SG unit for *NAT mode* or to connect directly to your ISP, refer to the User Manual on the SG CD (**\doc\UserManual.pdf**).

The SG unit ships with initial network settings of:

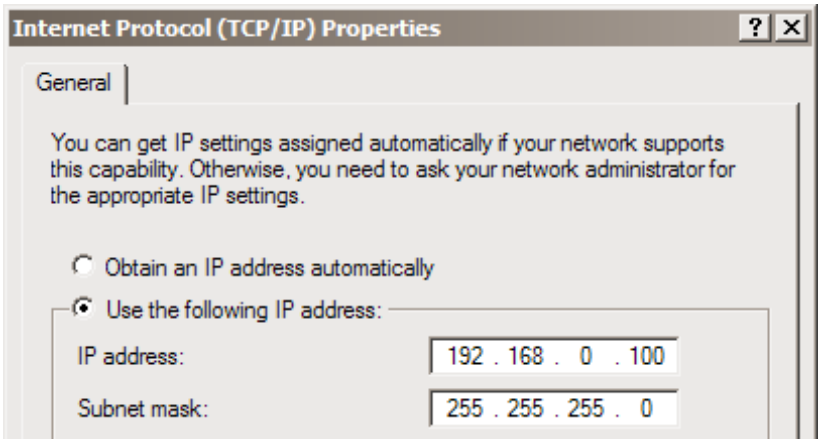
IP address:	**192.168.0.1**
Subnet mask:	**255.255.255.0**

Next, modify your PC's network settings to enable it to communicate with the SG unit.

Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections**.

Right click on **Local Area Connection** (or appropriate network connection for the newly installed PCI appliance) and select **Properties**.

Select **Internet Protocol (TCP/IP)** and click **Properties**.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 100
Subnet mask:
255 . 255 . 255 . 0

Select **Use the following IP address** and enter the following details:

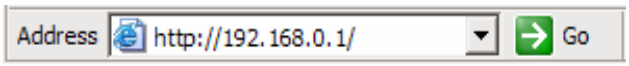
IP address: **192.168.0.100**

Subnet mask: **255.255.255.0**

Leave the **Default gateway** and **DNS server addresses** blank.

Set up the SG unit's password and network connection settings

Launch your web browser and navigate to **192.168.0.1**.



Select **Network Setup** from the **Networking** menu.

A log in prompt is displayed. Enter the initial user name and password for the SG unit:

User name: **root**

Password: **default**

Note

*If you are unable to connect to the management console at 192.168.0.1, or the initial username and password are not accepted, press the **Reset** button on the SG unit's rear panel **twice**, wait 20 – 30 seconds, and try again.*

*Pressing **Reset** twice within 2 seconds resets the SG unit to its factory default settings*

Enter and confirm a password for your SG unit. This is the password for the user **root**, the main administrative user account on the SG unit. It is therefore important that you choose a password that is hard to guess, and keep it safe.

Note

The new password takes effect immediately. You are prompted to enter it when completing the next step.

In the row labeled **Bridge**, click the **Modify** icon.

Note

The purpose of this step is to configure the IP address for the web management console. For convenience, this is generally a free IP address on your LAN.

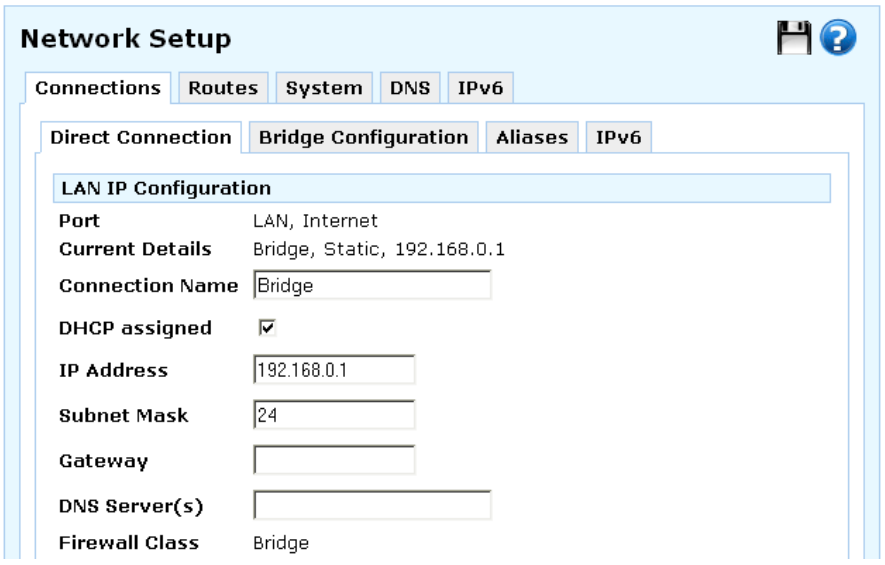
- ◇ If your LAN has a DHCP server running, you may set up the SG unit and your PC to obtain their network settings automatically. Proceed to *Automatic configuration*.
- ◇ Otherwise, you must manually specify network settings for both the SG unit and your PC. Proceed to *Manual configuration*.

Automatic configuration

Before continuing, ensure your DHCP server has two free leases. One is used for the web management console, the other for your PC.

Note

It is strongly recommended that you reserve the IP address to be used by the web management console using the SG unit's MAC address. In bridged mode, this is the top MAC address of the three displayed on the SG unit itself.



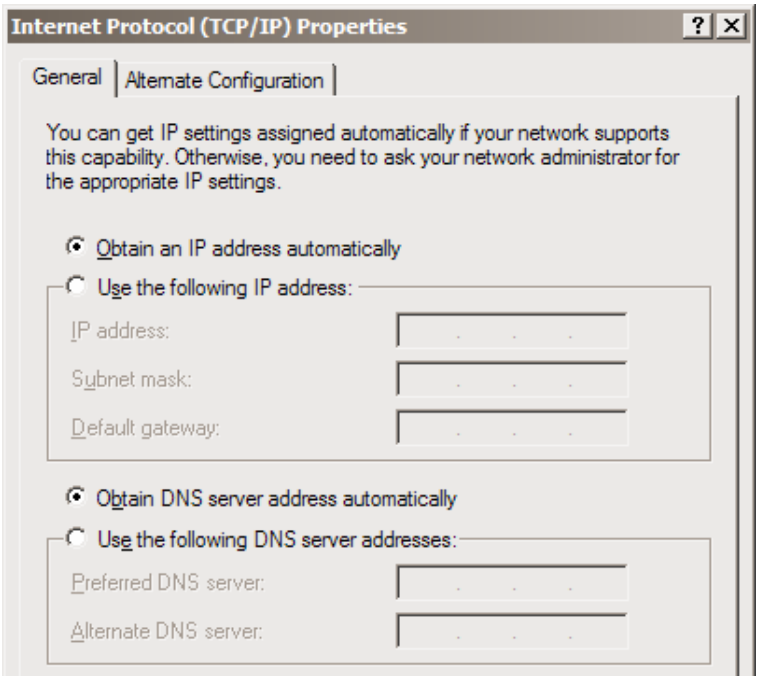
Check **DHCP assigned**. Anything in the **IP Address** and **Subnet Mask** fields is ignored.

Click **Update**.

Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections**.

Right click on **Local Area Connection** (or appropriate network connection for the newly installed PCI appliance) and select **Properties**.

Select **Internet Protocol (TCP/IP)** and click **Properties** and click **Properties**.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

Check **Obtain an IP address automatically**, check **Obtain DNS server address automatically** and click **OK**.

Attach your SG unit's Ethernet port to your LAN's hub or switch.

Quick setup is now complete.

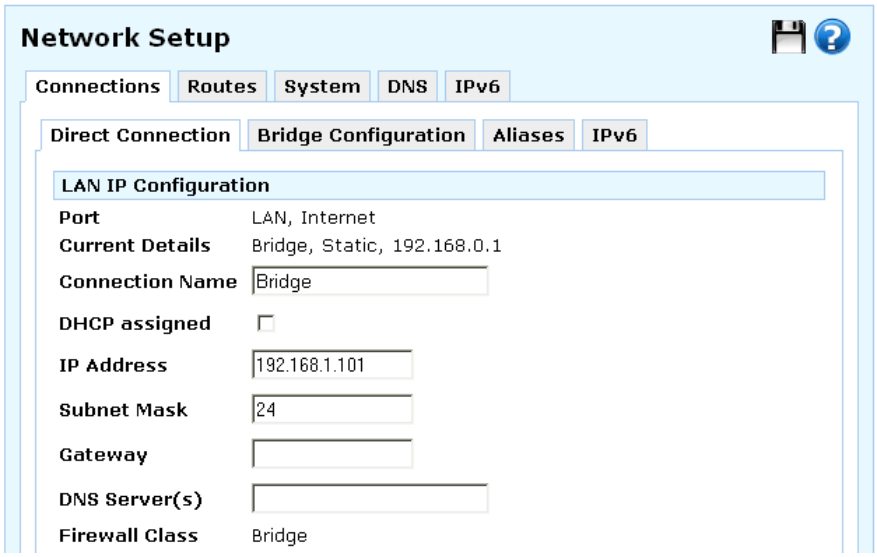
Manual configuration

Ensure you have two free IP addresses that are part of the subnet range of your LAN, and ensure you know your LAN's subnet mask, and the DNS server address and gateway address used by PCs on your LAN.

Note

Contact your network administrator if you are unsure of any of these settings.

The first IP address is used by the web management console



Enter this address as the **IP Address**, and the subnet mask for your LAN as the **Subnet mask**.

Ensure **DHCP assigned** is **unchecked**.

You may also enter one or more **DNS Server(s)** and a **Gateway** address to be used by the SG unit, not your PC, for access to the Internet. Typically this is not necessary, as only your PC needs to access the Internet.

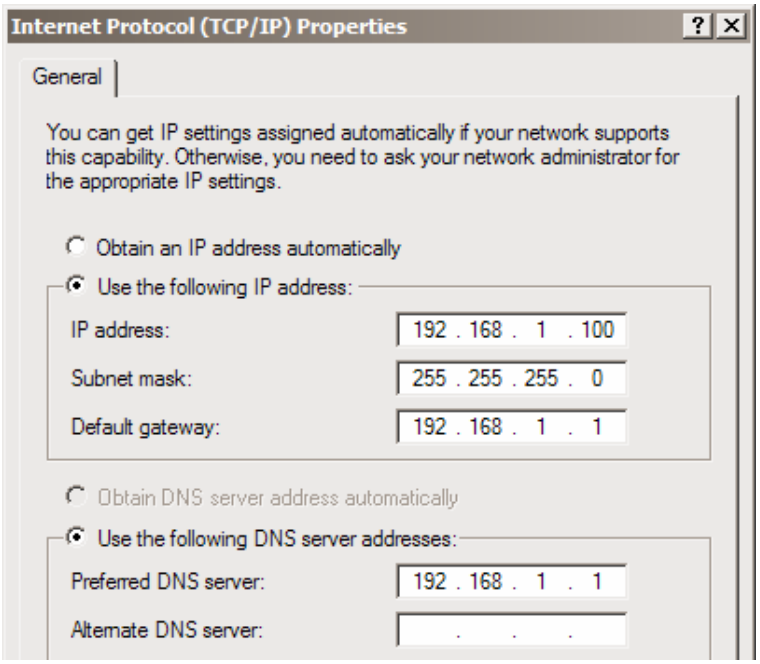
Click **Update**.

Next, configure your PC with the second IP address in the same manner you would as if it were connected to the LAN with a regular network interface card.

Click **Start** -> (**Settings** ->) **Control Panel** and double click **Network Connections**.

Right click on **Local Area Connection** (or appropriate network connection for the newly installed PCI appliance) and select **Properties**.

Select **Internet Protocol (TCP/IP)** and click **Properties**.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server:

Enter the following details:

- **IP address** is the second free IP addresses that is part of the subnet range of your LAN.
- **Subnet mask** is the subnet mask of your LAN.
- **Default gateway** is the IP address of your LAN's default gateway.
- **Preferred DNS server** is the IP address of the DNS server used by PCs on your LAN.

Click **OK**.

Attach your SG unit's Ethernet port to your LAN's hub.

Quick setup is now complete.

Disabling the reset button on your SG PCI appliance

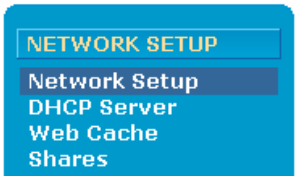
For convenience, the SG unit ships with the rear panel Reset button enabled. This allows the SG unit's configuration to be reset to factory defaults.

From a network security standpoint, it may be desirable to disable the Reset switch after initial setup has been performed. This is accomplished by removing the jumper linking *CON2* on the SG unit. This jumper is labeled *Remove Link to Disable Erase*.

The SG Management Console

The various features of your SG unit are configured and monitored using the management console. Follow the steps from the beginning of this chapter to set up your PC to access the management console.

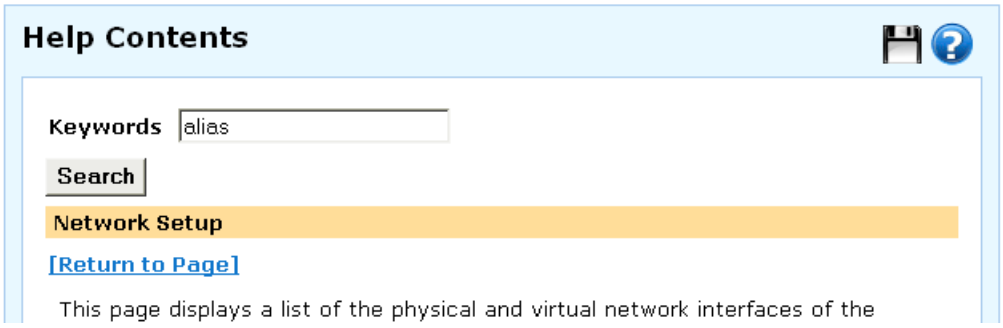
The main menu is displayed on the left hand side. Navigate your way around and get a feel for the SG unit's features by clicking the corresponding link in the main menu.



The remainder of this user manual is roughly divided into chapters based on the main menu section heading, e.g. *Network Setup*, *Firewall*, etc. Chapter sections roughly correspond to the menu items under each heading, e.g. *DHCP Server*, *Web Cache*.

Help

To access help for the current page, click the blue help icon on the top right hand side of the.screen.



Each field is described, along with acceptable input values where appropriate. To search the entire contents of the help system, enter search **Keywords** and click **Search**.

Backup/restore configuration

Hover your mouse over the black backup/restore icon on the top right hand side of the screen to display the date on which configuration changes were last backed up. Click the icon to backup or restore backed up configuration; see the *Backup/Restore* section of the chapter entitled *System* for details.

3. Network Setup

This chapter describes the **Network Setup** sections of the web management console. Here you can configure each of your SG unit's Ethernet, wireless and serial ports. It is accessed by clicking **Network Setup** under the **Network Setup** section of the main web management console menu.

The **QoS Traffic Shaping** and **IPv6** sections are also described towards the end of this chapter.

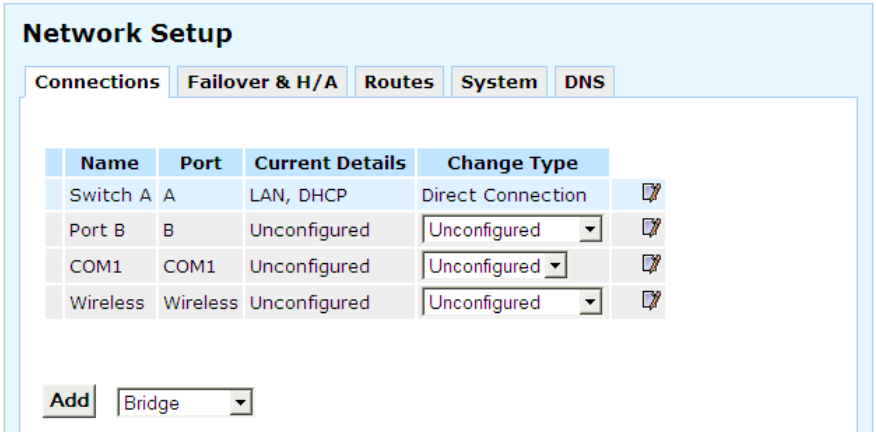
An Ethernet network interface may be configured to connect to your LAN, DMZ, an untrusted LAN, or the Internet as a primary, back-up or load-balacing connection. A serial port may be configured to provide remote dial-in access, or connect to the Internet as a primary or back-up connection. A wireless interface may be configured to connect to your LAN, DMZ or an untrusted LAN.

If you are using a SG gateway or rack mount appliance, the section *Set up the PCs on your LAN to access the Internet* in the chapter entitled *Getting Started* describes how to configure the PCs on your LAN to share the connection once your Internet connection has been established.

Configuring Connections

Under the **Connections** tab, each of your SG unit's network interfaces is displayed, alongside its physical **Port** name and the **Current Details** of its configuration.

Initially, all network interfaces are unconfigured, aside from a single LAN connection on the initial setup port (switch **A** on SG rack mount appliances, SG560, SG565 and SG580, the **LAN** port on other models).



A network interface is configured by selecting a connection type from the **Change Type** pull down menu. The current configuration can be viewed or modified by clicking the **Edit** icon. Clicking the **Delete** icon unconfigures a network interface; you are prompted to confirm this action.

Multifunction vs. Fixed-function Ports

Some SG units have network ports with labels corresponding to the port's function, i.e. **LAN**, **DMZ** and **Internet/WAN**. These are said to be *fixed-function ports*.

Alternatively, some SG units have network ports that are generically labeled, e.g. port **A**, port **B**, port **C**. These are said to be *multifunction ports*. This reflects the ability of these ports to perform many different functions, e.g. port **B** is not limited to connecting to the Internet only, it may be configured as a LAN connection.

Note

Before beginning configuration of multifunction ports, you should determine which function you are assigning to each of the ports.

Proceed to the section pertaining to your SG unit for information on its network ports and possible configurations.

SG710, SG710+: Multifunction Switches and Ports

SG rack mount appliances have a fixed-function LAN switch (switch **A**), and a multifunction switch (switch **B**) and two or four multifunction Ethernet ports (**C**, **D**, **E** and **F**).

Note

The switches' ports can not be configured individually; a switch is configured with a single function only (e.g., LAN switch, DMZ switch).

SG560, SG565 and SG580: Multifunction Ports

The SG560, SG565 and SG580 have generically named Ethernet ports (ports **A1**, **A2**, **A3**, **A4** and **B**). By default, switch **A** functions as a regular LAN switch, with network traffic passing freely between its ports. Typically, port **B** is used as your primary Internet connection.

However, switch **A**'s ports can be configured individually to perform separate functions, e.g. port **A2** can be a configured to connect to a second LAN, port **A3** can be configured as a DMZ port, and port **A4** can be configured as a secondary Internet connection.

These per-port configuration scenarios are accomplished using *VLANs* (virtual local area networks). For documentation concerning the advanced use of the VLAN capability of your SG unit, refer to the sections entitled *VLANs* and *Port based VLANs towards* the end of this chapter.

All Other SG Models: Fixed-function Ports

All other SG units have specifically labeled ports for specific functions.

The port labeled **LAN** may only perform the functions described in the section entitled *LAN Connection*, the port labeled **Internet** or **WAN** may only perform the functions described in the section entitled *Internet Connection*.

Note

*On SG570 and SG575 models, the **DMZ** port is special in that it may be configured with any kind of connection, i.e. LAN, DMZ, Guest or Internet. These connection types are discussed during the course of this chapter.*

Direct Connection

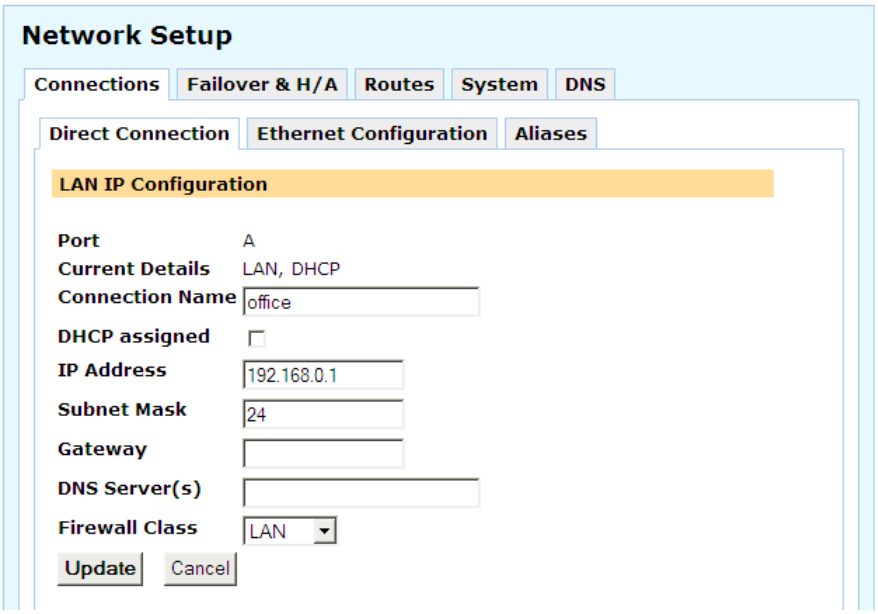
A direct connection is a direct IP connection to a network, i.e. a connection that does not require a modem to be established. This is typically a LAN, DMZ or Guest connection, but may also be an Internet connection. Network settings may be assigned statically, or dynamically by a DHCP server.

Note

Direct connections may be added to a network bridge, this is discussed in Bridging *later in this chapter.*

Network settings

Click the **Edit** icon of the interface your wish to modify.



To assign network settings statically, enter an **IP Address** and **Subnet Mask**. If you are using the SG unit in its default, network address translation mode, (see *Network address translation* in the *Advanced* section of this chapter), this is typically part of a private IP range, such as *192.168.0.1* / *255.255.255.0*. Ensure **DHCP assigned** is unchecked.

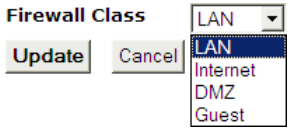
If required, enter a default **Gateway** out which to send outgoing traffic on this connection. For LAN connections, a default gateway is not generally necessary.

To have your SG unit obtain its LAN network settings from an active DHCP server on your local network, check **DHCP assigned**. Note that anything in the **IP Address**,**Subnet Mask** and **Gateway** fields are ignored.

You may also enter one or more **DNS servers**. Multiple servers may be entered separated by commas.

Firewall class

The **Firewall class** setting controls the basic allow/deny policy for this interface. Allowed network traffic is *accepted*, denied network traffic is *dropped*; this means network traffic is denied silently, no response such as "connection refused" is sent back to the originator of the traffic.



The following table details the policy associated with each firewall class. Note that VPN and Dial-In connections are by default assigned a firewall class of LAN.

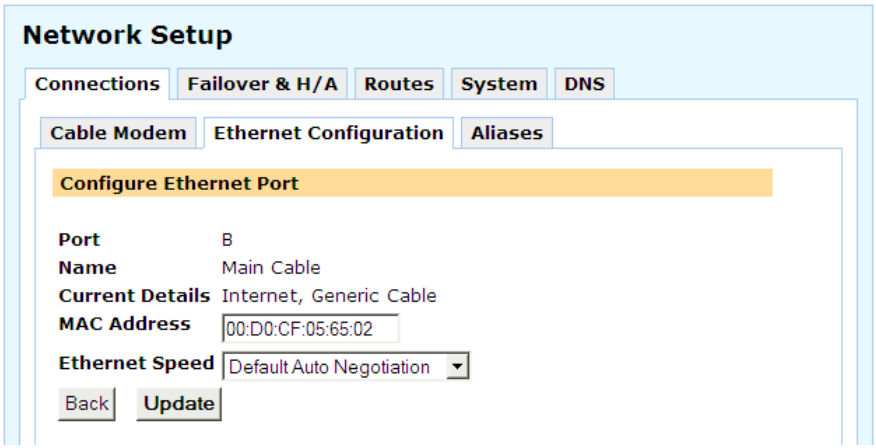
Incoming Interface	Outgoing Interface	Action
LAN	Any	Accept
VPN	Any	Accept
Dialin	Any	Accept
DMZ	Internet	Accept
DMZ	Any except Internet	Drop
Internet	Any	Drop
Guest	Any	Drop

For further discussion of DMZ and Guest networks, see the sections *DMZ Network* and *Guest Network* further on in this chapter.

Click **Update** to apply the new settings.

Ethernet configuration

Click the **Ethernet configuration** tab to modify the low level Ethernet configuration settings of an Ethernet network port.

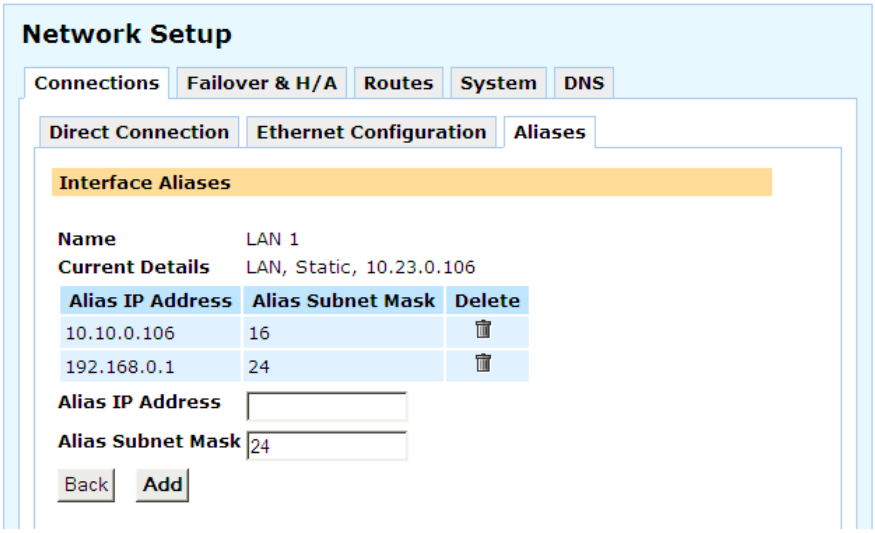


If an Ethernet port is experiencing difficulties auto-negotiating with another device, **Ethernet Speed** and duplex may be set manually.

On rare occasions it may be necessary to change the Ethernet hardware or **MAC Address** of your SG unit. The MAC address is a globally unique address and is specific to a single SG unit. It is set by the manufacturer and should not normally be changed. However, you may need to change it if your ISP has configured your ADSL or cable modem to only communicate with a device with a known MAC address.

Interface aliases

Interface aliases allow the SG unit to respond to multiple IP addresses on a single network interface. This is useful for when your ISP has assigned you a range of IP addresses to use with your Internet connection, or when you have more than one subnet connected to a single network interface.



For aliases on interfaces that have the DMZ or Internet firewall class, you must also setup appropriate **Packet Filtering** and/or **Port forwarding** rules to allow traffic on these ports to be passed onto the local network. See the chapter entitled *Firewall* for details.

IPv6

Click the **IPv6** tab to **Enable IPv6** for this connection.

Note

*To route and filter IPv6 traffic, you must also check the **Enable IPv6** option on the **IPv6** page; refer to the section entitled* IPv6 *towards the end of this chapter.*

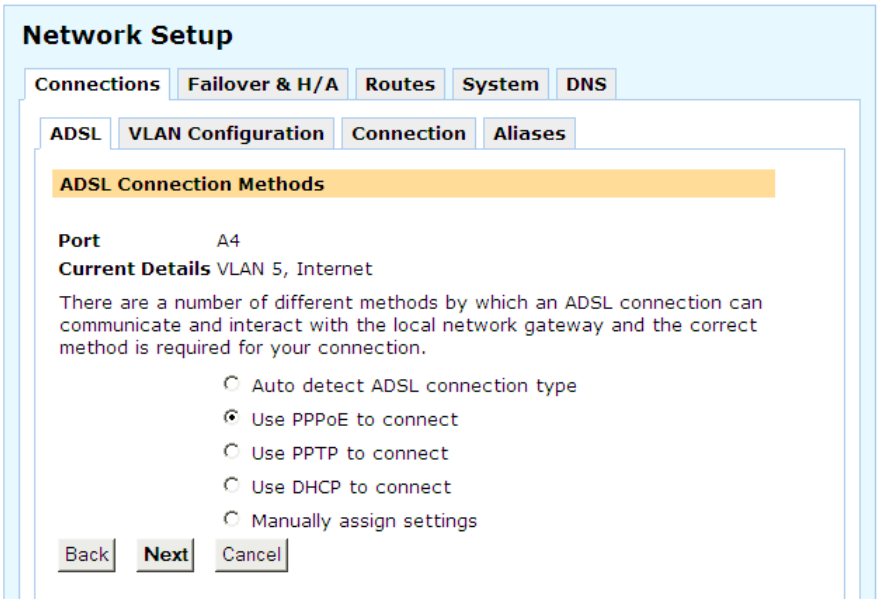
You may enter a site level aggregation value for this connection in **Site Level Aggregation**. It is used in the creation of a site local address and for routing IPv6 traffic on this connection. This setting is only available for LAN connections, and should be unique.

ADSL

To connect to the Internet using DSL, select **ADSL** from the **Change Type** pull down menu for the interface that connects to your DSL modem. ADSL connections have the interface firewall class of *Internet*.

If you have not already done so, connect the appropriate network port of your SG unit to your DSL modem. Power on the DSL modem and give it some time to initialize. If fitted, ensure the Ethernet link LEDs are illuminated on both the SG unit and DSL modem.

Do not continue until it has reached the *line sync* state and is ready to connect.



Select the connection method to use in establishing a connection to your ISP: **PPPoE**, **PPTP**, **DHCP**, or **Manually Assign Settings**.

Note

*Use **PPPoE** if your ISP uses username and password authentication to access the Internet. Use **PPTP** if your ISP has instructed you to make a dial-up VPN connection to the Internet. Use **DHCP** if your ISP does not require a username and password, or your ISP instructed you to obtain an IP address dynamically. If your ISP has given you an IP address or address range, you must **Manually Assign Settings**.*

If you are unsure, you may let the SG unit attempt to **Auto detect ADSL connection type**. Note that the SG unit is unable to detect the **PPTP** connection type.

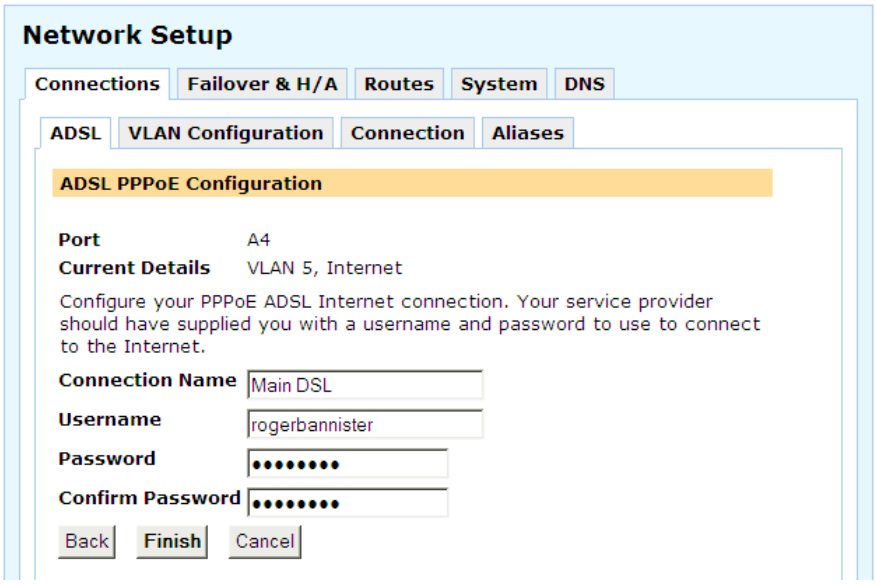
Note

If autodetection fails, it may also be because your DSL modem is misconfigured for your connection type, or your DSL service has not yet been provisioned by your telco.

Click **Next** to continue.

PPPoE

To configure a **PPPoE** or **PPPoA** connection, enter the user name and password provided by your ISP. You may also enter a descriptive **Connection Name** if you wish. Click **Finish**.



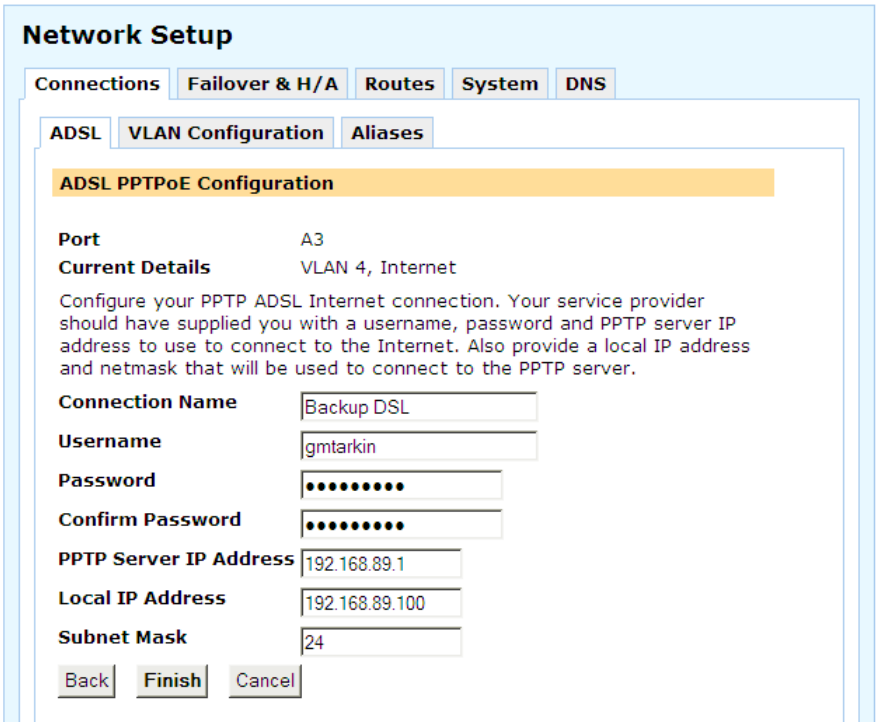
Note

For PPPoE/PPPoA connections, ensure your DSL modem is set to operate in bridged mode. Typically, for PPPoE connections, your DSL modem must be set to use LLC *multiplexing/encapsulation. For PPPoA connections, your DSL modem must be set to use* VC*-based multiplexing/encapsulation.*

By default, PPPoE connections are treated as “always on” and are kept up continuously. Alternatively, you may choose to only bring the connection up when PCs on the LAN, DMZ or Guest network (via a VPN tunnel) are trying to reach the Internet. For instructions, refer to the section entitled *Dial on Demand* further on in this chapter. As DSL connections are not generally metered by time, this is not generally necessary.

PPTP

To configure a **PPTP** connection to your ISP, enter the **PPTP Server IP Address** and a **Local IP Address** and **Netmask** for the SG network port through which you are connecting to the Internet.



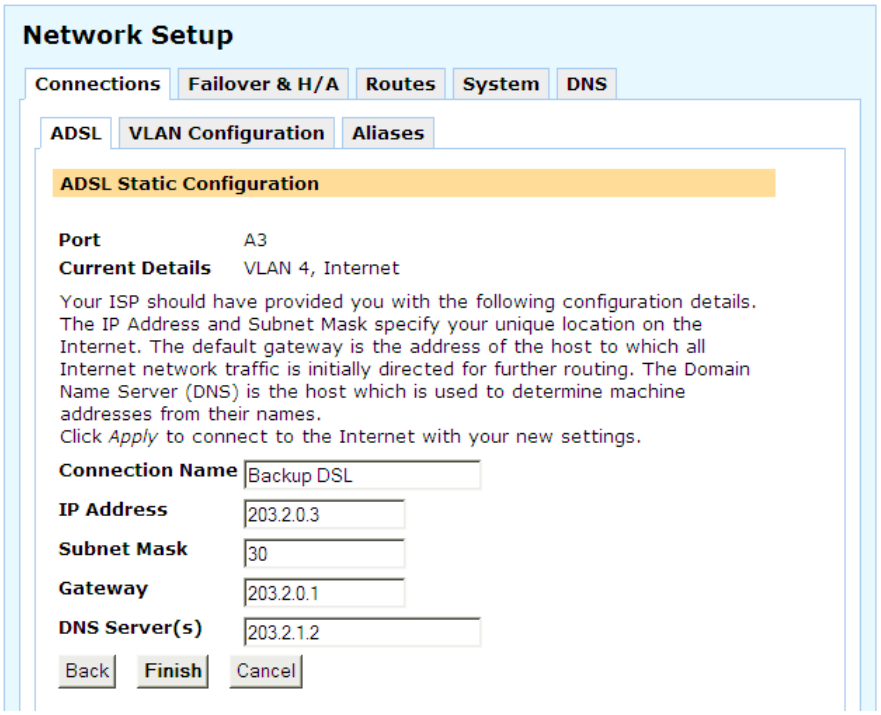
The **Local IP address** is used to connect to the PPTP server and is not typically your real Internet IP address. You may also enter a descriptive **Connection Name** if you wish. Click **Finish** or **Update**.

DHCP

DHCP connections may require a **Hostname** to be specified, but otherwise all settings are assigned automatically by your ISP. You may also enter a descriptive **Connection Name** if you wish. Click **Finish** or **Update**.

Manually assign settings

For **Manually Assign Settings** connections, enter the **IP Address**, **Subnet mask**, the **Gateway** and the **DNS Address** provided by your ISP.


Network Setup
Connections
Failover & H/A
Routes
System
DNS
ADSL
VLAN Configuration
Aliases
ADSL Static Configuration
Port
A3
Current Details
VLAN 4, Internet
Your ISP should have provided you with the following configuration details. The IP Address and Subnet Mask specify your unique location on the Internet. The default gateway is the address of the host to which all Internet network traffic is initially directed for further routing. The Domain Name Server (DNS) is the host which is used to determine machine addresses from their names.
Click Apply to connect to the Internet with your new settings.
Connection Name
Backup DSL
IP Address
203.2.0.3
Subnet Mask
30
Gateway
203.2.0.1
DNS Server(s)
203.2.1.2
Back
Finish
Cancel

The latter two settings are optional, but are generally required for normal operation. Multiple DNS addresses may be entered separated by commas. You may also enter a descriptive **Connection Name** if you wish. Click **Finish** or **Update**.

Connection (dial on demand)

You may choose to bring up a PPPoE/PPPoA DSL, dialout or ISDN connection only when PCs on the LAN, DMZ or Guest network (via a VPN tunnel) are trying to reach the Internet and disconnect again when the connection has been idle for a specified period. This is known as *dial on demand*, and is particularly useful when your connection is metered by time.

Click the **Edit** icon then the **Connection** tab for the connection for which you wish to enable dial on demand.

Check **Dial on Demand**. **Idle Time (minutes)** is the number of minutes the SG unit waits after the connection becomes idle before disconnecting. **Max Connection Attempts** specifies the number of times the SG unit attempts to connect should the dial up connection fail. This is useful to prevent the situation where an incorrectly entered username and password or expired account leads to a large phone bill. **Time between redials (seconds)** is the time to wait between such reconnection attempts.

Ethernet configuration

See the section entitled *Ethernet configuration* under *Direct Connection*.

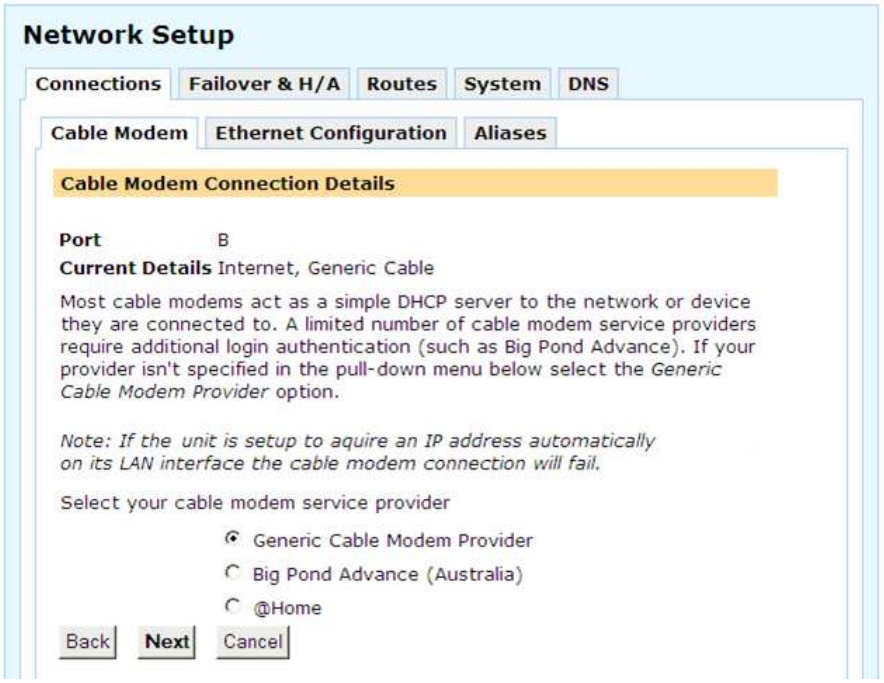
Aliases

See the section entitled *Aliases* under *Direct Connection*.

Cable Modem

To connect to the Internet using a cable Internet service, select **Cable Modem** from the **Change Type** pull down menu for the interface that connects to your cable modem. Cable Modem connections have the interface firewall class of *Internet*.

If you have not already done so, connect the appropriate network port of your SG unit to your cable modem. Power on the cable modem and give it some time to initialize. If fitted, ensure the Ethernet link LEDs are illuminated on both the SG unit and cable modem.


Network Setup
Connections
Failover & H/A
Routes
System
DNS
Cable Modem
Ethernet Configuration
Aliases
Cable Modem Connection Details
Port B
Current Details Internet, Generic Cable
Most cable modems act as a simple DHCP server to the network or device they are connected to. A limited number of cable modem service providers require additional login authentication (such as Big Pond Advance). If your provider isn't specified in the pull-down menu below select the Generic Cable Modem Provider option.
Note: If the unit is setup to aquire an IP address automatically on its LAN interface the cable modem connection will fail.
Select your cable modem service provider
Generic Cable Modem Provider
Big Pond Advance (Australia)
@Home
Back
Next
Cancel

Select your cable ISP from the list and click **Next**. If your provider does not appear, select **Generic Cable Modem Provider**. You may enter a descriptive **Connection Name** if you wish. For cable modem providers other than **Generic**, enter your user name and password or hostname. Click **Finish** or **Update**.

Ethernet configuration

See the section entitled *Ethernet configuration* under *Direct Connection*.

Aliases

See the section entitled *Aliases* under *Direct Connection*.

Dialout and ISDN

To connect to the Internet using a regular dialup or ISDN service, select **Dialout** from the **Change Type** pull down menu for the interface that connects to your dialup modem or ISDN TA. Dialout and ISDN connections have the interface firewall class of *Internet*.

Note

To connect to an ISDN line, the SG unit requires an intermediate device called a Terminal Adapter (TA). A TA connects into your ISDN line and has either a serial or Ethernet port that is connected to your SG unit. Do not plug an ISDN connection directly in to your SG unit.

Enter the **Phone Number(s) to Dial** and the **Username** and **Password** provided by your ISP. The **DNS Server(s)** setting is optional, your ISP may automatically assign DNS servers when the connection is established. You may enter a descriptive **Connection Name** if you wish. Click **Finish** or **Update**.

Note

If your ISP has provided multiple phone numbers, you may enter them separated with commas. Use **\,** *to send a comma (pause) to your modem, e.g. if you need to dial* 0 *to get an outside line from behind a PABX, and your ISP's number is* 1234567*, the* ***Phone Number*** *field may look like:* 0\,\,\,1234567

By default, Dialout/ISDN connections are treated as “always on” and is kept up continuously. Alternatively, you may choose to only bring the connection up when PCs on the LAN, DMZ or Guest network (via a VPN tunnel) are trying to reach the Internet. For instructions, refer to the section entitled *Dial on Demand* further on in this chapter.

Port settings

If necessary, you may set the SG unit’s serial port **Baud** rate and **Flow Control**. This is not generally necessary.

Static addresses

The majority of ISPs dynamically assign an IP address to your connection when you dialin. However some ISPs use pre-assigned static addresses. If your ISP has given you a static IP address, click the **Static Addresses** tab and enter it in **My Static IP Address** and enter the address of the ISP gateway in **ISP Gateway IP Address**.

Aliases

See the section entitled *Aliases* under *Direct Connection*.

Connection (dial on demand)

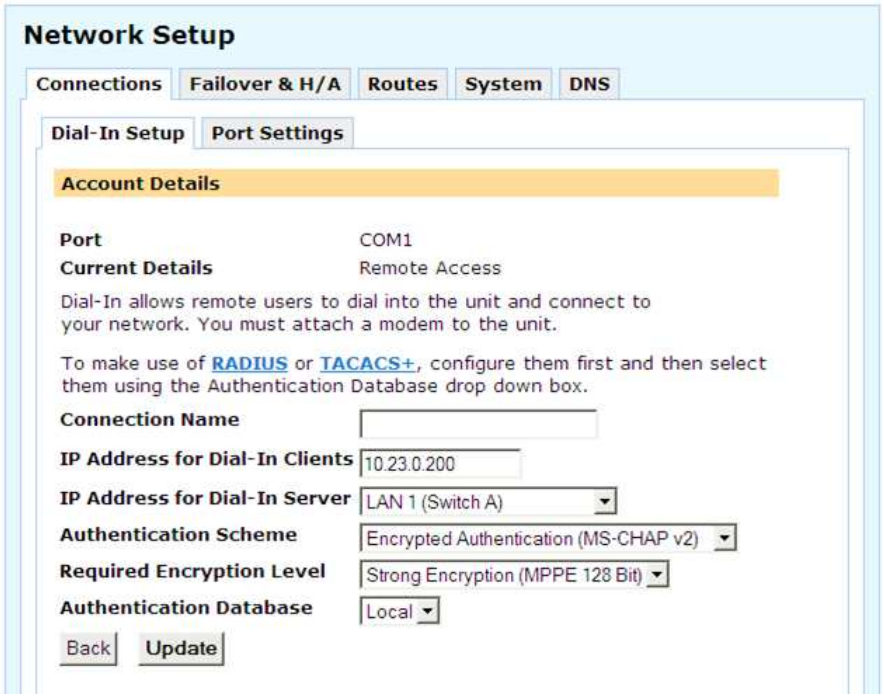
See the section entitled *Connection (dial on demand)* under *ADSL*.

Dialin

A remote user may dial directly to a modem connected to SG unit’s serial port. Once connected and authenticated, the user has access to network resources as if they were a local user on the LAN. This may be useful for remote administration of your SG unit, or for telecommuting.

Dialin setup

Select **Dialin** from the **Change Type** pull down menu for the interface that connects to the dialup modem to answer incoming calls.



If you wish, you may enter a descriptive **Connection Name**.

Enter a free **IP Address for Dial-In Clients**, this must be a free IP address from the network (typically the LAN) that the remote user is assigned while connected to the SG unit.

If you have configured several network connections, select the one that you want to connect remote users to from the **IP Address for Dial-In Server** pull down menu. This is typically a LAN interface or alias.

Select the weakest **Authentication Scheme** to accept, access is denied to remote users attempting to connect using an authentication scheme weaker than this. They are described below, from strongest to weakest.

- **Encrypted Authentication (MS-CHAP v2):** The strongest type of authentication to use. This is the recommended option.
- **Encrypted Authentication (MS-CHAP):** This is not a recommended encryption type and should only be used for older dialin clients that do not support MS-CHAP v2.
- **Weakly Encrypted Authentication (CHAP):** This is the weakest type of encrypted password authentication to use. It is not recommended that clients connect using this as it provides very little password protection. Also note that clients connecting using CHAP are unable to encrypt traffic.

- **Unencrypted Authentication (PAP):** This is plain text password authentication. When using this type of authentication, the client passwords are transmitted un-encrypted.

Select the **Required Encryption Level**, access is denied to remote users attempting to connect not using this encryption level. Using **Strong Encryption (MPPE 128 Bit)** is recommended.

Select the **Authentication Database**. This allows you to indicate where the list of valid clients can be found. You can select from the following options:

- **Local:** Use the local database defined on the **Local Users** tab of the **Users** page. You must enable the **Dialin Access** option for the individual users that are allowed dialin access.
- **RADIUS:** Use an external RADIUS server as defined on the **RADIUS** tab of the **Users** page.
- **TACACS+:** Use an external TACACS+ server as defined on the **TACACS+** tab of the **Users** page.

Note

See the Users *section of the chapter entitled* System *for details on adding user accounts for dialin access, and configuring the SG unit to enable authentication against a RADIUS or TACACS+ server.*

Click **Update**.

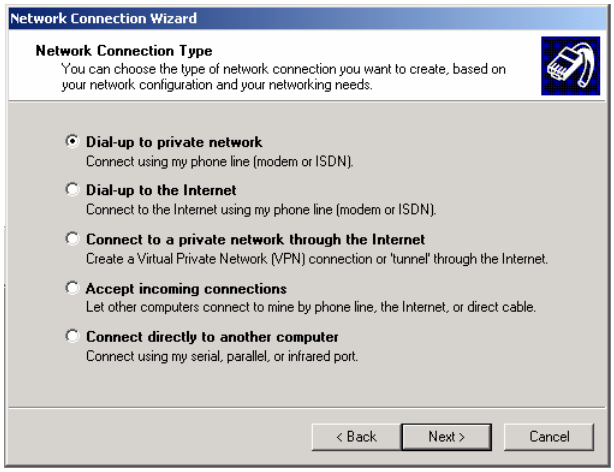
Connecting a dialin client

Remote users can dial in to the SG unit using the standard Windows **Dial-Up Networking** software or similar. The following instructions are for Windows 2000/XP.

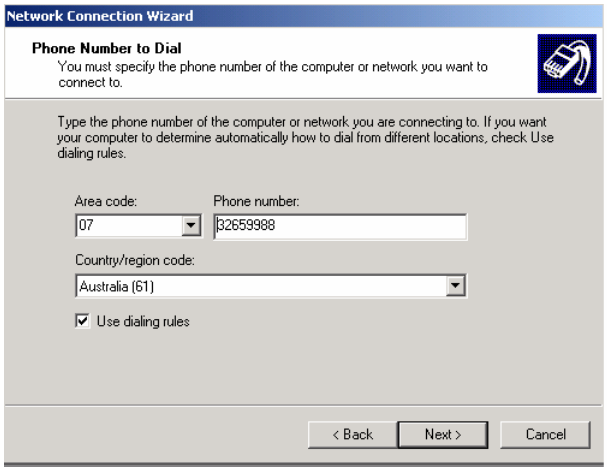
Click **Start**, **Settings**, **Network and Dial-up Connections** and select **Make New Connection**. The network connection wizard guides you through setting up a remote access connection:

Network Connection Wizard
Welcome to the Network Connection Wizard
Using this wizard you can create a connection to other computers and networks, enabling applications such as e-mail, Web browsing, file sharing, and printing.
To continue, click Next.
< Back
Next >
Cancel

Click **Next** to continue.

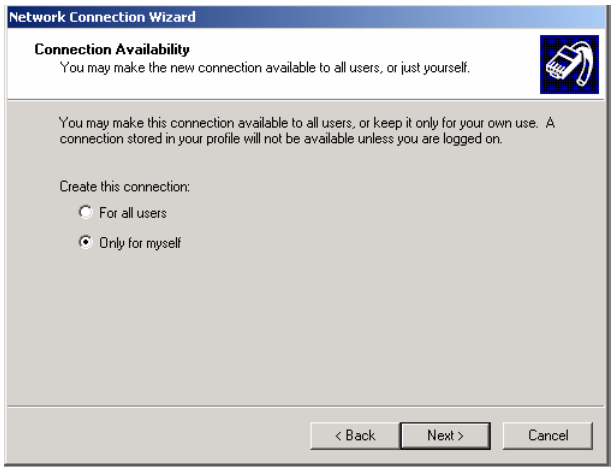

Network Connection Wizard
Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.
Dial-up to private network
Connect using my phone line (modem or ISDN).
Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).
Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.
Connect directly to another computer
Connect using my serial, parallel, or infrared port.
< Back
Next >
Cancel

Select **Dial-up to private network** as the connection type and click **Next** to continue.


Network Connection Wizard
Phone Number to Dial
You must specify the phone number of the computer or network you want to connect to.
Type the phone number of the computer or network you are connecting to. If you want your computer to determine automatically how to dial from different locations, check Use dialing rules.
Area code:
Phone number:
07
32659988
Country/region code:
Australia (61)
Use dialing rules
< Back
Next >
Cancel

Tick **Use dialing rules** to enable you to select a country code and area code. This feature is useful when using remote access in another area code or overseas.

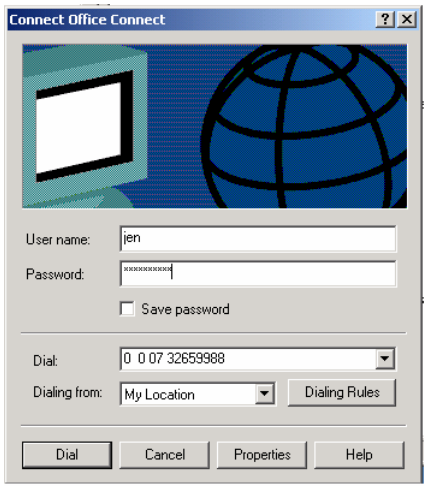
Click **Next** to continue.


Network Connection Wizard
Connection Availability
You may make the new connection available to all users, or just yourself.
You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.
Create this connection:
For all users
Only for myself
< Back
Next >
Cancel

Select the option **Only for myself** to make the connection only available for you. This is a security feature that does not allow any other users who log onto your machine to use this remote access connection:

Network Connection Wizard
Completing the Network Connection Wizard
Type the name you want to use for this connection:
Office Connect
To create this connection and save it in the Network and Dial-up Connections folder, click Finish.
To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.
Add a shortcut to my desktop
< Back
Finish
Cancel

Enter a name for the connection and click **Finish** to complete the configuration. Check **Add a shortcut to my desktop** to add an icon for the remote connection to the desktop.



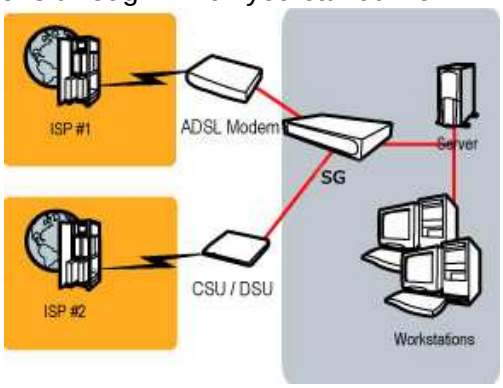
To launch the new connection, double-click on the new icon on the desktop. The remote access login screen appears as in the next figure. If you did not create a desktop icon, click **Start** -> **Settings** -> **Network and Dial-up Connections** and select the appropriate connection. Enter the username and password set up for the SG unit dialin account.

Failover, Load Balancing and High Availability

Note

SG gateway and rack mount appliances only.

The SG unit supports a wide range of configurations through which you can utilize multiple Internet connections, and even multiple SG units, to help ensure Internet availability in the event of service outage or heavy network load.



The following Internet availability services are provided by the SG unit. They may be configured individually, or in combination.

- *Internet Failover*: configuring a back up, redundant Internet connection (or connections) that is only established should the primary link lose connectivity

- *Load Balancing:* establishing another Internet connection (or connections) concurrently with the primary link, for spreading network load over multiple connections

- *High Availability:* installing a back up, redundant SG unit to monitor the status of the primary unit, coming online and becoming the Internet gateway for your network should the primary SG unit fail

Note

SG unit models SG300, SG530 and SG550 are limited to Internet availability configurations using a single broadband Internet connection and a single dialout or ISDN connection.

Configure Internet connections

Configure all Internet connections to use in conjunction with the SG unit's Internet availability services. Secondary and tertiary Internet connections are configured in the same manner as the primary Internet connection, as detailed in the sections entitled *Direction Connection*, *ADSL*, *Cable Modem*, and *Dialout/ISDN* earlier in this chapter.

Note

If you are using a SG unit model SG560, SG565 or SG580, you may want to skip ahead to the section entitled Port Based VLANs *later in this chapter, for information on establishing multiple broadband connections.*

Once the Internet connections have been configured, specify the conditions under which the Internet connections are established.

Internet Failover

Note

If you have configured your SG560, SG565 or SG580's switch as separate ports, and are establishing multiple PPPoE ADSL Internet connections using two or more of these ports, it is important that each port is connected to a remote device with a unique MAC address. This is almost definitely the case if each of the Internet connections are through different ISPs, otherwise you may have to request this specifically from your ISP.

If this is not possible, set each of the ADSL modems to routing *or* NAT *rather than* bridged *mode. Typically this means the ADSL modem terminates the PPPoE connection, and the SG appliance is configured with DHCP or manually assigned settings, using the ADSL modem as a gateway.*

SG units support three connection levels. A *connection level* consists of one or more Internet connections. When all primary connections are functioning as expected, the primary connection level is deemed to be up.

If one or more of the primary connections should fail, the SG unit drops back to the secondary connection level. This typically involves bringing up a secondary Internet connection, until the primary Internet connection or connections become available again.

You may also optionally configure the tertiary failover level. If one or more of the secondary connections should fail, the SG unit drops back to the tertiary connection level. This is typically a "last resort" dialup link to the Internet, but may be any kind of network connection. The primary connection level and secondary connection level are tested in turn, until one becomes available.

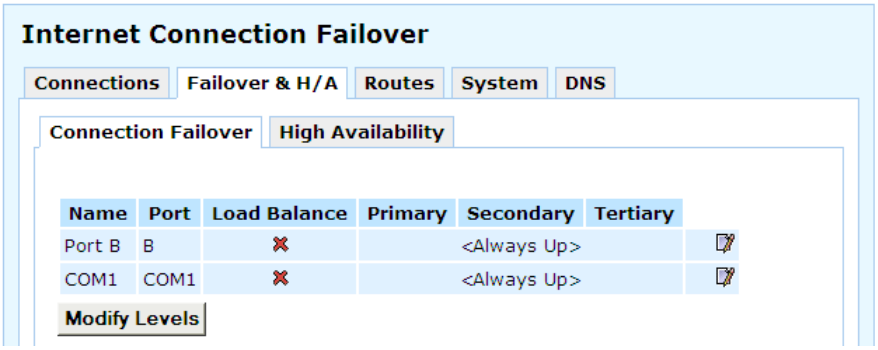
Note

Internet failover is not stateful, i.e. any network connections that were established through the failed primary connection must be re-established through the secondary connection.

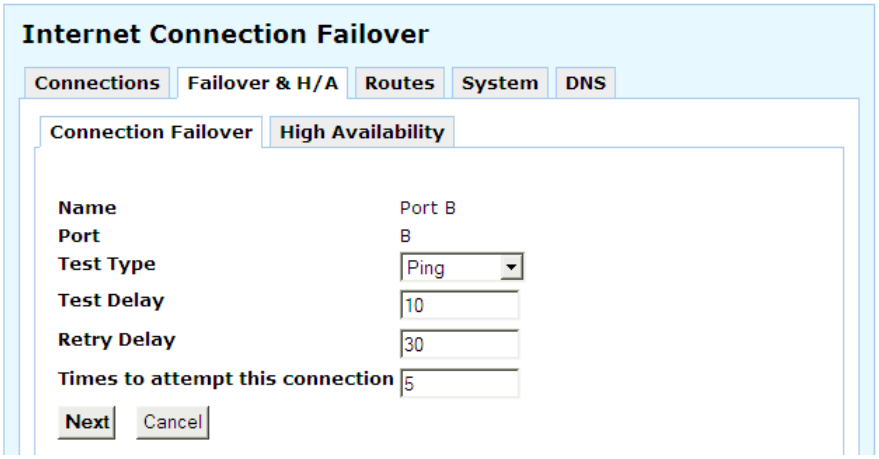
Edit connection parameters

The first step of configuring failover is to set failover parameters for each connection. These parameters specify how to test whether a connection is up and functioning correctly.

On the **Network Setup** page, click the **Failover & H/A** tab. A list of the connections that you have configured is displayed under the **Connection Failover** tab, alongside ticks and crosses. The ticks and crosses indicate how the connection behaves at each failover level, this is discussed further in the section entitled *Modify failover levels (primary, secondary, tertiary)*.



Click the **Edit** icon next to the connection to edit its failover parameters. The **Name** and **Port** of this connection is displayed, along with several options.



Select a **Test Type**. The **Ping** test is usually appropriate.

- **Ping** sends network traffic to a remote host at regular intervals, if a reply is received the connection is deemed to be up.

- **Custom** *(advanced users only)* allows you to enter a custom console command to run to determine whether the connection is up. This is typically a script you have written and uploaded to the SG unit.

- **Always Up** means no test is performed, and Internet failover is disabled for this connection.

If you wish, you may fine tune the timeouts for the failover test, however the defaults are usually suitable.

- **Test Delay** is the number of seconds to wait after starting this connection before testing whether it is functioning correctly, a longer delay is used for connection types that are slow to establish, such as dialout.

- **Retry Delay** is the number of seconds to wait after a connection test fails before re-attempting the test.

- **Times to attempt this connection** is the number of times to try a connection before giving up. Once the SG unit has given up trying this connection, manual intervention is required to re-establish it.

Click **Next** to configure settings specific to the **Test Type**.

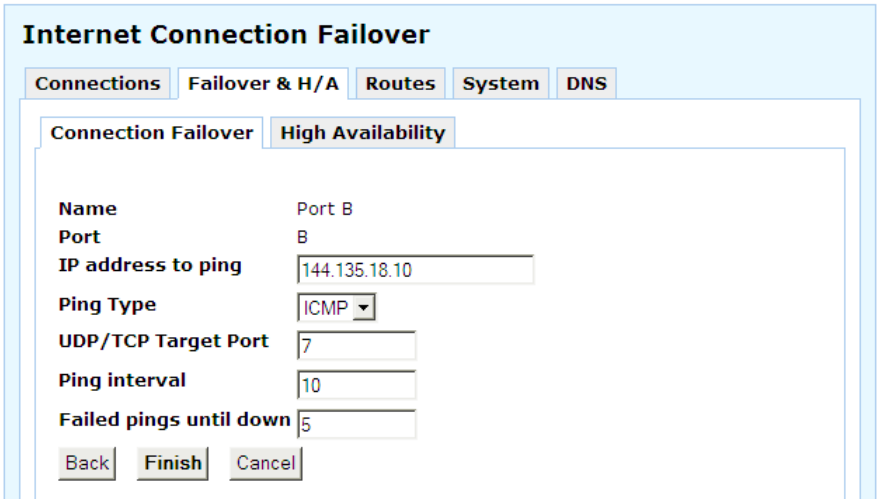
- If you selected a **Test Type** of **Always Up**, no further configuration is required. Skip ahead to *Modify failover levels (primary, secondary, tertiary)*.

- If you selected **Custom**, enter the custom **Test Command** that is used to test the connection, e.g.: `myscript 5 10 ping -c 1 -I $if_netdev 15.1.2.3`

  Note

  *If the **Test Command** exits with a return code of zero (0), the test is deemed to have passed and the connection is considered up. Otherwise, the connection is considered down. Also note that* `$if_netdev` *is replaced with the name of the network interface on which the test is being run, e.g.* `ppp0`*.*

- If you selected **Ping**, enter an **IP Address to Ping**. Ensure you choose a host on the Internet that can be contacted reliably and responds to pings. You can check whether you can ping a host under **Diagnostics** -> **Network Tests** -> **Ping Test**.



Ping Interval is the time to wait in between sending each ping, **Failed Pings** is the number of missed ping replies before this connection attempt is deemed to have failed.

Click **Finish**.

Modify failover levels (primary, secondary, tertiary)

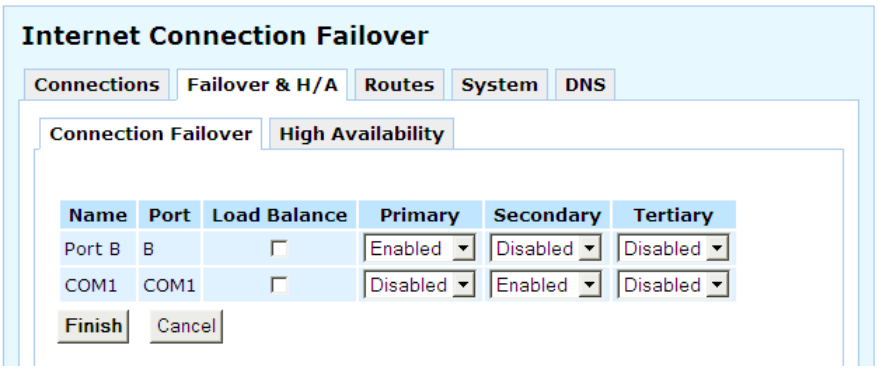
The second and final step of configured Internet failover is associating Internet connections with and primary, secondary and optionally tertiary connection levels.

Recall that a connection level is one or more connections. These connections may be marked as **Required** or **Enabled**. Internet connections that are marked **Disabled** are not part of this connection level. A connection level is deemed to be up when all connections marked **Required** at that level are up, and at least one connection (marked **Required** or **Enabled**) at that level is up.

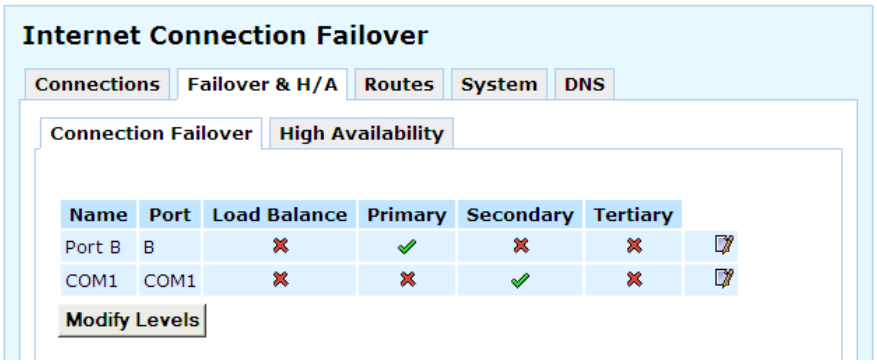
On the **Network Setup** page, click the **Failover & H/A** tab, then **Modify Levels**. A table is displayed listing each of the connections alongside a drop down box for each connection level.

Note

*If a connection is marked **<Always Up>**, you must edit its connection parameters as described by the previous section before it can be associated with a connection level.*



First, configure the **Primary** connection level. If you have a single Internet connection only, setting it to **Enabled** or **Required** has the same effect. For failover to occur, you must then configure at least the secondary connection level. Click **Finish**.



This returns you to the main **Connection Failover** page. You'll notice that ticks and crosses are display alongside each connection, describing how they are configured for each connection level. A red cross means **Disabled**, a green ticket means **Enabled** and a green tick with a small red plus means **Required**,

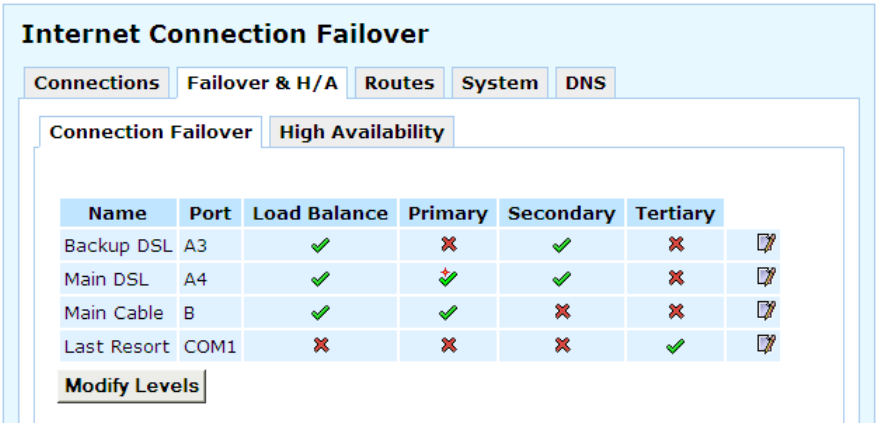
Internet Load Balancing

Once you have configured two or more Internet connections, you may enable Internet load balancing. Load balancing may be used in conjunction with Internet failover, or on its own.

Note

If you have configured your SG560, SG565 or SG580's switch as separate ports, and are establishing multiple PPPoE ADSL Internet connections using two or more of these ports, it is important that each port is connected to a remote device with a unique MAC address. This is almost definitely the case if each of the Internet connections are through different ISPs, otherwise you may have to request this specifically from your ISP.

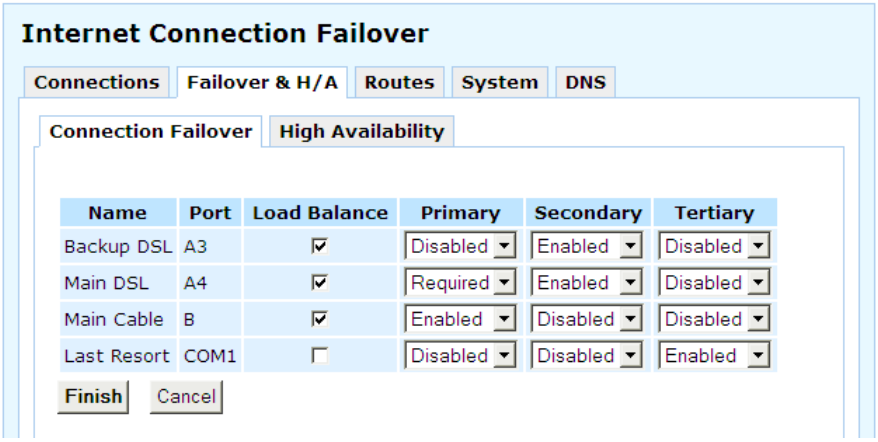
If this is not possible, set each of the ADSL modems to routing *or* NAT *rather than* bridged *mode. Typically this means the ADSL modem terminates the PPPoE connection, and the SG appliance is configured with DHCP or manually assigned settings, using the ADSL modem as a gateway.*



The Internet connections need not be the same, e.g. you can perform load balancing between a PPPoE ADSL connection on one network port, and a Cable Internet connection on the other.

Enabling load balancing

Under the **Failover & H/A** tab, click **Modify Levels**.



Check **Load Balance** for each connection to enable for load balancing. Click **Finish**.

Note

Load balancing settings are not specified for each failover level; load balancing occurs when any two or more load balancing connections are up.

Limitations of load balancing

Load balancing works by alternating outgoing traffic across Internet connections in a round robin manner. It does not bond both connections together to work as one link, e.g. it does not bond two 512 Kbit/s links to function as a single 1 Mbit/s link.

Total bandwidth and available bandwidth are *not* taken into account when choosing a connection on which to send outgoing traffic.

When an internal client makes a connection to a server on the Internet, this and subsequent connections between the the internal client and remote server are confined to the one Internet connection to ensure connections are not broken.

If a second internal client makes a connection to the same remote server, it may or may not go across the same link, depending on which Internet connection is next to be selected in the round robin process.

VPN connections such as IPSec or PPTP tunnels are confined to a single Internet connection, as they are a single connection (that encapsulate other connections).

Load balancing is not performed for incoming traffic. This scenario can be addressed using other solutions such as round robin DNS to alternate incoming connections between the two links.

High Availability

Just as Internet failover keeps a redundant Internet connection on stand-by should the primary connection fail, high availability allows a second SG unit to provide network connectivity should the primary SG appliance fail.

High availability is accomplished with two SG units on the same network segment which provide some identical network service (such as Internet access) to other hosts on that network segment.

A "floating" IP address (e.g. 192.168.1.1) is configured as an alias on the interface on that network segment on exactly one of the devices. This is done via simple negotiation between the two devices such that one device has the IP address (master) and one does not (slave).

Note

This floating IP address is in addition to the primary IP addresses of the two devices (e.g. 192.168.1.2 and 192.168.1.3) for the interface on the network segment.

The floating IP address and primary IP addresses of the two devices need not be part of the same network (e.g. 192.168.1.0/24), but typically will be.

As far as hosts on the network are concerned, they may use either a device's primary IP address to address a particular device, or the floating IP address to use whichever device is currently up.

For example, a host may have its default gateway assigned as the floating IP address.

Note

High availability does not perform stateful failover between SG units, i.e. any network connections that were established through the failed device must be re-established through the new master device.

Enabling high availability

On each of the devices, select the **Failover & H/A**, then the **High Availability** tab.

You may use either the supplied script, */bin/highavaild*, to manage the shared address, or you may write your own script, possibly based on */bin/highavaild*.

Note

/bin/highavaild is a Tcl script. The SG unit uses TinyTcl, which provides a fairly extensive subset of regular Tcl's features. Documentation is available from: http://tinytcl.sourceforge.net/

If you are using the supplied /bin/*highavaild* script, enter a command similar to the following as the **Start Command** on both devices. **Stop Command** and **Test Command** are not required in the basic scenario.

```
/bin/highavaild [-d] [-n] [-a alias] ipaddr &
```

ipaddr is the floating IP address. You do not need to manually configure this address on either unit, the script handles this internally.

alias is an alias interface name, such as *eth0:9*, on which to configure *ipaddr* when this device is the master. If you do not specify an alias, the script automatically selects the *eth0:9*.

-d enables extra debug output to the sytem log.

-n disables the *High Availability* or *HA* LED, if it is present on your SG unit.

Note

Normally the script controls the HA LED to indicate the status of HA, however if two or more highavaild scripts are used for different interfaces, only one is able to control the LED.

Advanced configurations

The supplied script is intended as a starting point for more advanced High Availability configurations.

By default, a device is considered "up" and a candidate to become the master if it is powered up and connected to the network segment. If you wish to have the device become master only if some other service is available (say, an Internet connection), a **Test** command may be added that checks for the availability of that resource and returns 0 if it is available.

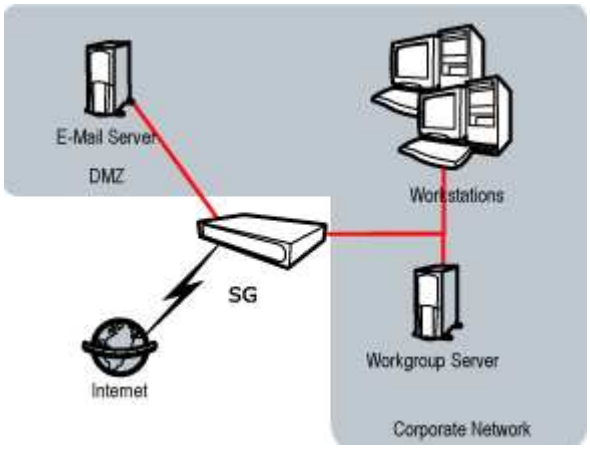
/bin/highavaild may be configured any any interface, however if used on a non-LAN interface, appropriate packet filter rules need to be configured to allow traffic via the floating IP address (see the *Packet Filtering* section of the chapter entitled *Firewall*).

DMZ Network

Note

Not available on the SG300, SG530, SG550 or SG PCI appliances.

A DMZ (de-militarized zone) is a physically separate LAN segment, typically used to host servers that are publically accessible from the Internet.



Servers on this segment are isolated to provide better security for your LAN. If an attacker compromises a server on the LAN, then the attacker immediately has direct access to your LAN. However, if an attacker compromises a server in a DMZ, they are only able to access other machines on the DMZ.

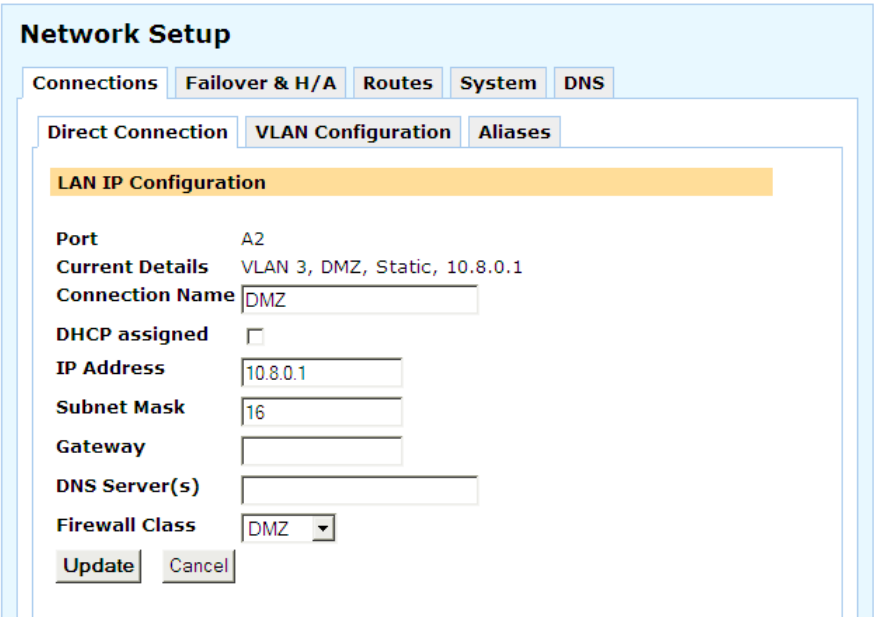
In other words, by default the SG unit blocks network traffic originating from the DMZ from entering the LAN. Additionally, any network traffic originating from the Internet is blocked from entering the DMZ and must be specifically allowed before the servers become publically accessible. Network traffic originating from the LAN is allowed into the DMZ and network traffic originating from the DMZ is allowed out to the Internet, however.

The section *Services on the DMZ Network* discusses how to allow certain traffic from the Internet into the DMZ. To allow public access to the servers in the DMZ from the Internet, this step must be performed. You may also allow certain network traffic originating from the DMZ into the LAN, however this is not usually necessary.

By default, machines on the DMZ network have addresses in a private IP address range, such as *192.168.1.0* / *255.255.255.0* or *10.1.0.0* / *255.255.0.0*. Real world addresses may be used on the DMZ network by by unchecking **Enable NAT from DMZ interfaces to Internet interfaces** under the **Advanced** tab. See the *Network address translation* section later in this chapter for further information.

Configuring a DMZ connection

Select **Direct Connection** from the **Configuration** pull down box of the network port to be connected to the DMZ. Enter appropriate IP address settings and select **DMZ** from **Firewall Class** pull down menu.



Configuring a **Direct Connection** is described in detail in the section entitled *Direct Connection* towards the beginning of this chapter.

Services on the DMZ network

Once you have configured the DMZ connection, configure the SG unit to allow access to services on the DMZ. There are two methods of allowing access.

If the servers on the DMZ have public IP addresses, you need to add packet filtering rules to allow access to the services. See the section called *Packet Filtering* in the chapter entitled *Firewall*.

If the servers on the DMZ servers have private IP addresses, you need to port forward the services. See the section called *Incoming Access* in the chapter entitled *Firewall*. Creating port forwarding rules automatically creates associated packet filtering rules to allow access. However, you can also create custom packet filtering rules if you wish to restrict access to the services.

You may also want to configure your SG unit to allow access from servers on your DMZ to servers on your LAN. By default, all network traffic from the DMZ to the LAN is dropped. See the section called *Packet Filtering* in the chapter entitled *Firewall*.

Guest Network

Note

Not available on the SG300, SG530, SG550 or SG PCI appliances.

The intended usage of Guest connections is for connecting to a Guest network, i.e. an untrusted LAN or wireless networks. Machines connected to the Guest network must establish a VPN connection to the SG unit in order to access the LAN, DMZ or Internet.

By default, you can configure the SG's DHCP server to hand out addresses on a Guest network, and the SG's VPN servers (IPSec, PPTP, etc.) to listen for connections from a Guest network and establish VPNs. Aside from this, access to any LAN, DMZ or Internet connections from the Guest network is blocked.

If you want to allow machines on a Guest network direct access to the Internet, LAN or DMZ without first establishing a VPN connection, add packet filtering rules to allow access to services on the LAN or Internet as desired. See the *Packet Filtering* section in the chapter entitled *Firewall* for details.

Warning

Caution is advised before allowing machines on a Guest network direct access to your LAN. This may make it a lot easier for an attacker to compromise internal servers.

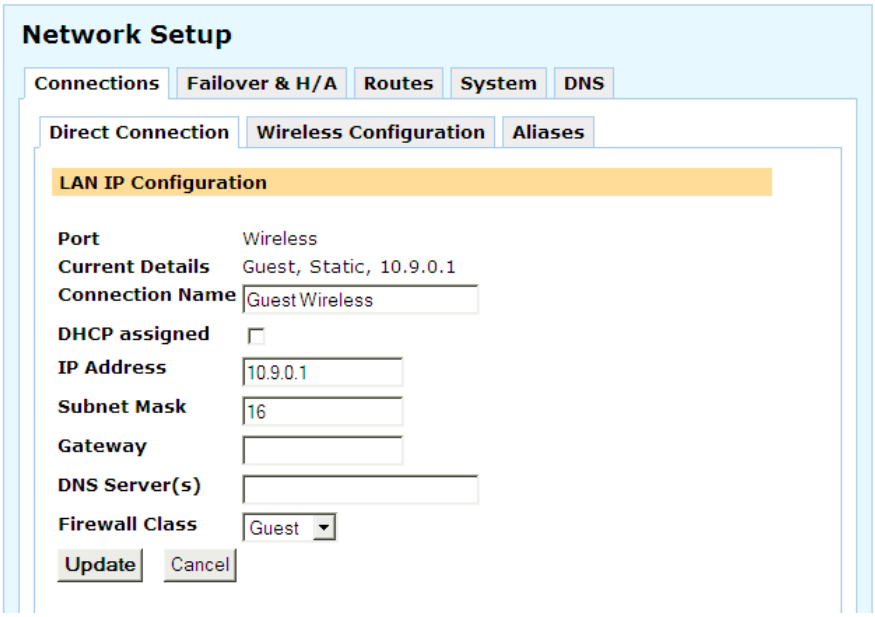
Caution is also advised before allowing machines on a Guest network direct access to the Internet, particularly in the case of Guest wireless networks. This may result in unauthorized use of your Internet connection for sending spam, other malicious or illegal activities, or simply Internet access at your expense.

Machines on the Guest network typically have addresses in a private IP address range, such as *192.168.2.0* / *255.255.255.0* or *10.2.0.0* / *255.255.0.0*. For network address translation (NAT) purposes, the Guest connection is considered a LAN interface, i.e. the NAT checkboxes for **LAN interfaces** under **Advanced** modify settings for both LAN connections and Guest connections. See the *Network address translation* section later in this chapter for further information.

A Guest connection is established by selecting **Direct Guest** or **Bridged Guest** from the **Configuration** pull down box of the network port to be connected to the Guest network.

Configuring a Guest connection

Select **Direct Connection** from the **Configuration** pull down box of the network port to be connected to the Guest network. Enter appropriate IP address settings and select **Guest** from **Firewall Class** pull down menu.



Configuring a **Direct Connection** is described in detail in the section entitled *Direct Connection* towards the beginning of this chapter.

Wireless

Note

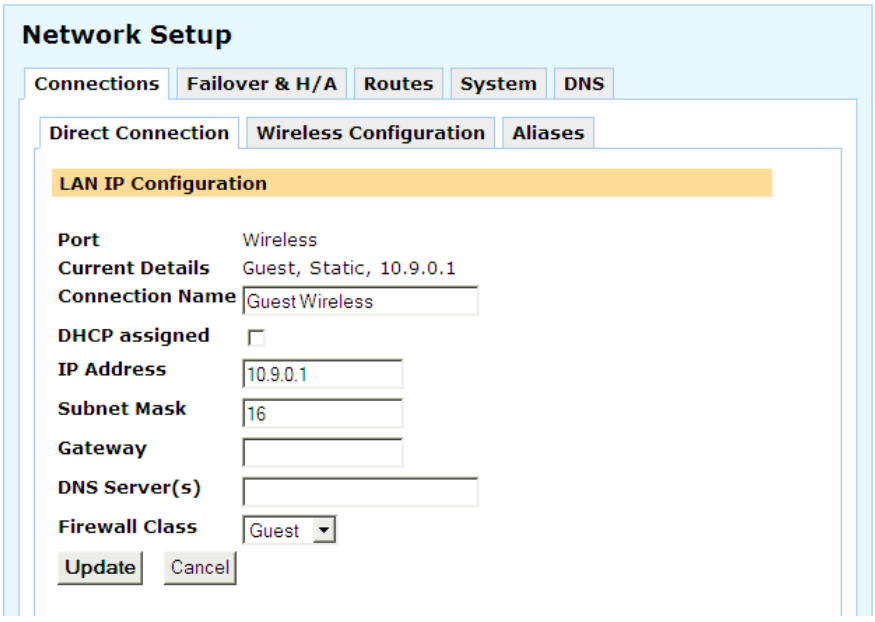
SG565 only.

The SG unit's wireless interface may be configured as a wireless access point, accepting connections from 802.11b (11 Mbit/s) or 802.11g (54 Mbit/s) capable wireless clients.

Typically, the SG unit's wireless interface is configured in one of two ways; with strong wireless security (WPA) to bridge wireless clients directly onto your LAN, or with weak wireless security as a Guest connection. The latter requires wireless clients to establish a VPN tunnel on top of the wireless connection to access the LAN, DMZ and Internet, to compensate for the security vulnerabilities WEP poses.

Configuring a wireless connection

Select **Direct Connection** from the **Change Type** pull down box of the wireless network interface. Enter appropriate IP address information for the wireless network, and from the **Firewall Class** pull down menu, select whether your wireless network is a **Guest**, **DMZ**, **LAN** or **Internet** connection.



Warning

We strongly recommend that the wireless interface be configured as a LAN connection ***only if*** *wireless clients are using WPA-PSK encryption/authentication. This is discussed in further detail later in this section.*

Configuring a **Direct Connection** is described in detail in the section entitled *Direct Connection* towards the beginning of this chapter. See the sections *DMZ Network* and *Guest Network* earlier in this chapter for further discussion of these network types.

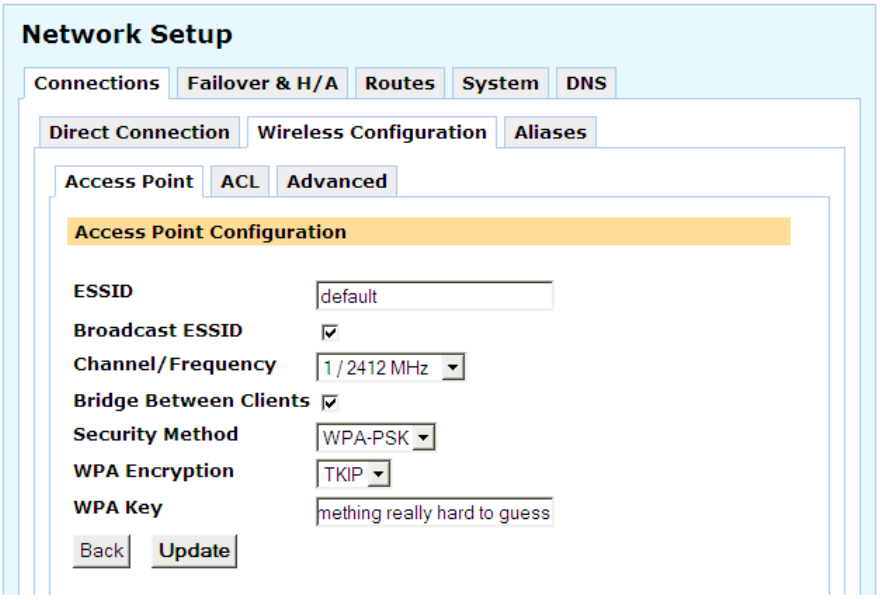
In addition to connection configuration, you may also configure wireless access point, access control list (ACL) and advanced settings. These settings are described in the following section.

Note

A walkthrough for configuring your SG unit to bridge wireless clients directly onto your LAN is provided in the section entitled Connecting wireless clients*, towards the end of the* Wireless *section.*

Basic wireless settings

To edit basic wireless settings, click the **Edit** icon alongside the **Wireless** network interface, click the **Wireless Configuration** tab, then the **Access Point** tab. Each of the fields is discussed below.



ESSID: (Extended Service Set Identifier) The ESSID is a unique name that identifies a wireless network. This value is case sensitive, and may be up to 32 alphanumeric characters.

Broadcast ESSID: Enables broadcasting of the ESSID. This makes this wireless network visible to clients that are scanning for wireless networks. Choosing not to broadcast the ESSID should not be considered a security measure; clients can still connect if they know the ESSID, and it is possible for network sniffers to read the ESSID from other clients.

Channel/Frequency: Select the operating frequency or channel for the wireless network. Changing to a different channel may give better performance if there is interference from another access point.

Bridge Between Clients: This setting enables the access point to forward packets between clients at the wireless level, i.e. wireless clients are able to “see” each other. This means that packets between wireless clients are not restricted by the firewall. Note that if you disable this setting, but you still want to allow access between clients in the firewall, you usually also need to configure each client to route to other clients via the access point.

Wireless security

Encryption and authentication settings for your wireless network are configured under **Access Point**. Fields vary based on the security method you choose.

If **Security Method** is set to **None**, any client is allowed to connect, and there is no data encryption.

Warning

If you use this setting, then it is highly recommended that you configure wireless interface as a Guest connection, disable bridging between clients, and only allow VPN traffic over the wireless connection.

WEP security method

WEP (Wired Equivalent Privacy) allows for 64 or 128 bit encryption.

Warning

The WEP protocol has known security flaws, so it is recommended that you configure the wireless interface as a Guest connection, disable bridging between clients, and only allow VPN traffic over the wireless connection.

WEP Authentication:

- **Open System:** Allow any client to authenticate. Since clients must still have a valid WEP key in order to send or receive data, this setting does not make the WEP protocol less secure, and is the recommended setting.
- **Shared Key:** Clients must use the WEP key to authenticate.

Warning

*Due to flaws in the authentication protocol, this method reduces the security of the WEP key. It is recommended that you use **Open System** authentication instead.*

- **Open System or Shared Key:** Allows clients to authenticate using either of the above two methods.

WEP Key Length: This sets the length of the WEP keys to be entered below. It is recommended to use 128 bit keys if possible.

WEP Key: Enter up to 4 encryption keys. These must be either 10 hexadecimal digits (0 – 9, A – F) for 64 bit keys, or 26 hexadecimal digits for 128 bit keys. You must also select one of the 4 keys to be the default transmit key.

WPA-PSK (aka WPA-Personal) security method

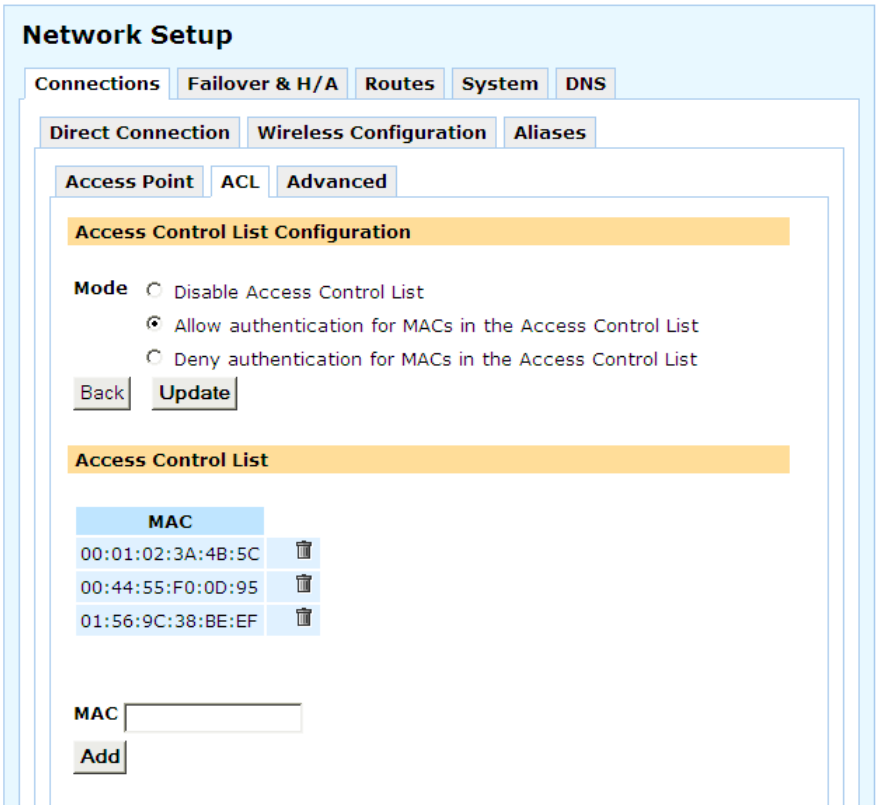
WPA-PSK (Wi-Fi Protected Access Preshared Key) is an authentication and encryption protocol that fixes the security flaws in WEP. This is the recommended security method.

WPA Encryption: Select the encryption algorithm, either **TKIP** (Temporary Key Integrity Protocol) or **AES** (Advanced Encryption Standard).

WPA Key: Enter the WPA preshared key, which can be either 8 to 63 ASCII characters, or 64 hexadecimal characters.

ACL (Access Control List)

To edit access control list settings, click the **Edit** icon alongside the **Wireless** network interface, click the **Wireless Configuration** tab, then the **ACL** tab.



When the **Access Control List** is disabled (**Disable Access Control List**), any wireless client with the correct ESSID (and encryption key if applicable) can connect to the wireless network. For additional security, you can specify a list of MAC addresses (network hardware addresses) to either allow or deny.

Select **Allow authentication for MACs in the Access Control List** to disallow all but the MAC addresses you specify, or **Deny authentication for MACs in the Access Control List** to allow all but the MAC address you specify. Click **Update**.

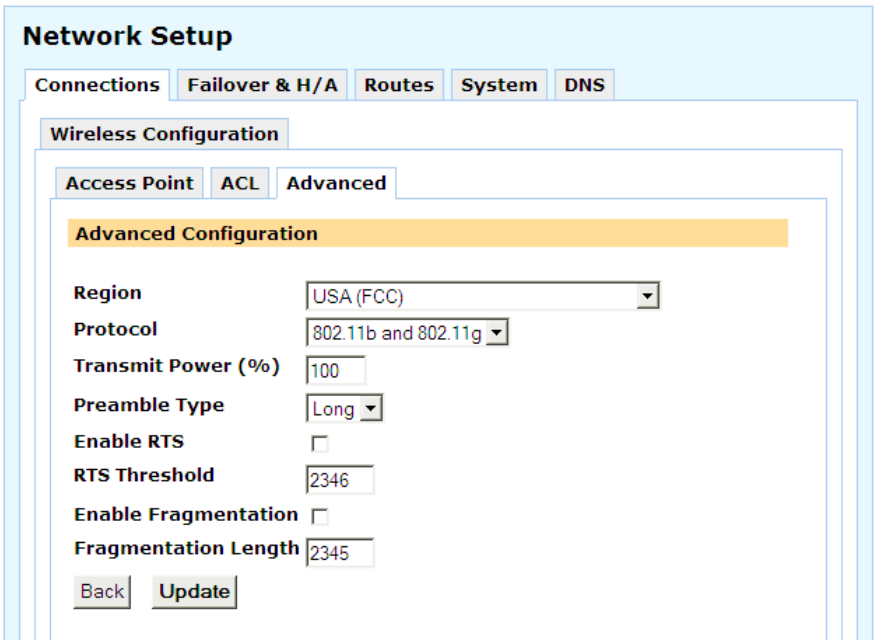
Enter a **MAC** to allow or deny and click **Add**. A **MAC** may be removed from the list by clicking the corresponding **Delete** icon.

Warning

This is only a weak form of authentication, and does not provide any data privacy (encryption). MAC addresses may be forged relatively easily.

Advanced

To edit access control list settings, click the **Edit** icon alongside the **Wireless** network interface, click the **Wireless Configuration** tab, then the **Advanced** tab.



Region: Select the region in which the access point is operating. This restricts the allowable frequencies and channels. If your region is not listed, select a region that has similar regulations.

Protocol:

- **802.11b only:** Wireless clients can only connect using 802.11b (11 Mbit/s). Note that most wireless clients which support 802.11g also support 802.11b.
- **802.11g only:** Wireless clients can only connect using 802.11g (54 Mbit/s). Wireless clients that only support 802.11b are unable to connect.
- **802.11b and 802.11g:** Both 802.11b and 802.11g wireless clients can connect.

Transmit Power (%): Select the transmit power for the access point. Decreasing the power reduces the range of the network. This reduces interface caused to other nearby access points, and limit the range from which clients can connect.

Preamble Type: The preamble is part of the physical wireless protocol. Using a short preamble can give higher throughput. However, some wireless clients may not support short preambles.

Enable RTS: RTS (Request to Send) is used to negotiate when wireless clients can transmit.

If you have two wireless clients that are out of range of each other, but both still within range of the access point, they may both attempt to transmit at the same time, causing a collision. Enabling RTS avoids these collisions, and thus increases performance.

RTS incurs an overhead for transmitting, so enabling it when it is not needed decreases performance. Since the access point is in range of all wireless clients, you would not normally enable RTS for an access point.

RTS Threshold: The minimum packet size for which RTS is enabled. Collisions are less likely for smaller packets, and so the overhead of using RTS for these may not be worthwhile.

Enable Fragmentation: Normally, when a packet has an error, the entire packet must be retransmitted. If packet fragmentation is enabled, the packet is split up into smaller fragments, and thus only the fragment that has an error needs to be retransmitted, which increases performance.

Fragmentation incurs an overhead per fragment, so enabling it when it is not needed decreases performance.

Fragmentation Length: Using smaller fragments decreases the amount that is retransmitted when there is an error, but it also increases the total overhead for each packet.

Beacon Interval (ms): Beacon frames are used to coordinate the wireless network. Sending beacon frames more often (i.e.using a lower becon interval) increases responsiveness, but decreases performance due to higher overheads.

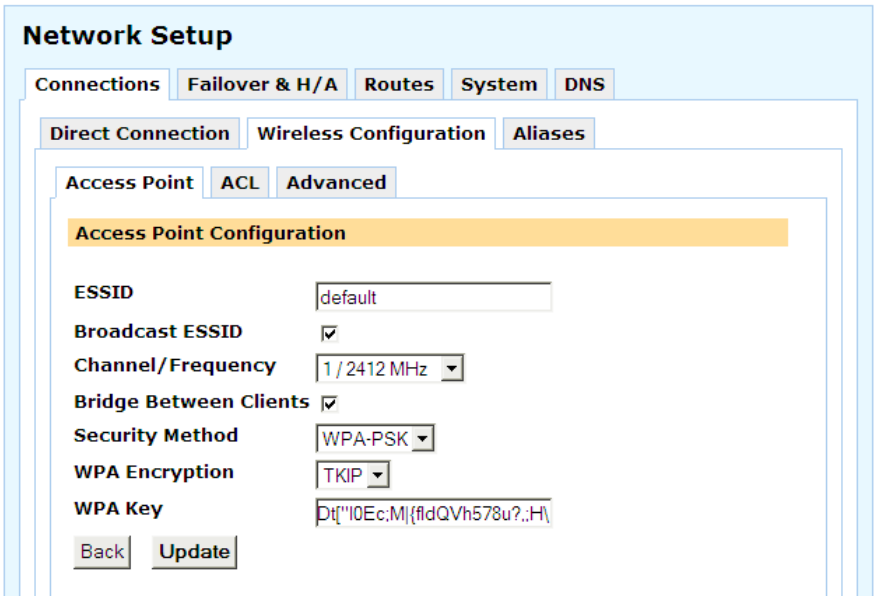
DTIM Interval (beacons): Specify how often a Delivery Traffic Indication Message is sent. A DTIM is periodically included in the beacon frame. A DTIM is used to indicate to clients in power saving mode that there are packets for them to receive. Sending a DTIM more often increases responsiveness for clients in power saving mode, but uses more power since the clients must stay awake longer.

Connecting wireless clients

The following steps detail how to configure your SG unit to bridge between its wireless and LAN interfaces. The result of this configuration would be similar to attaching a wireless access point in bridge mode to one of the SG unit's LAN ports. Individual settings and fields are detailed earlier in the *Wireless* section.

The wireless and wired LAN interfaces share a single IP address, in this example the wireless interface shares the existing IP address of the wired LAN interface.

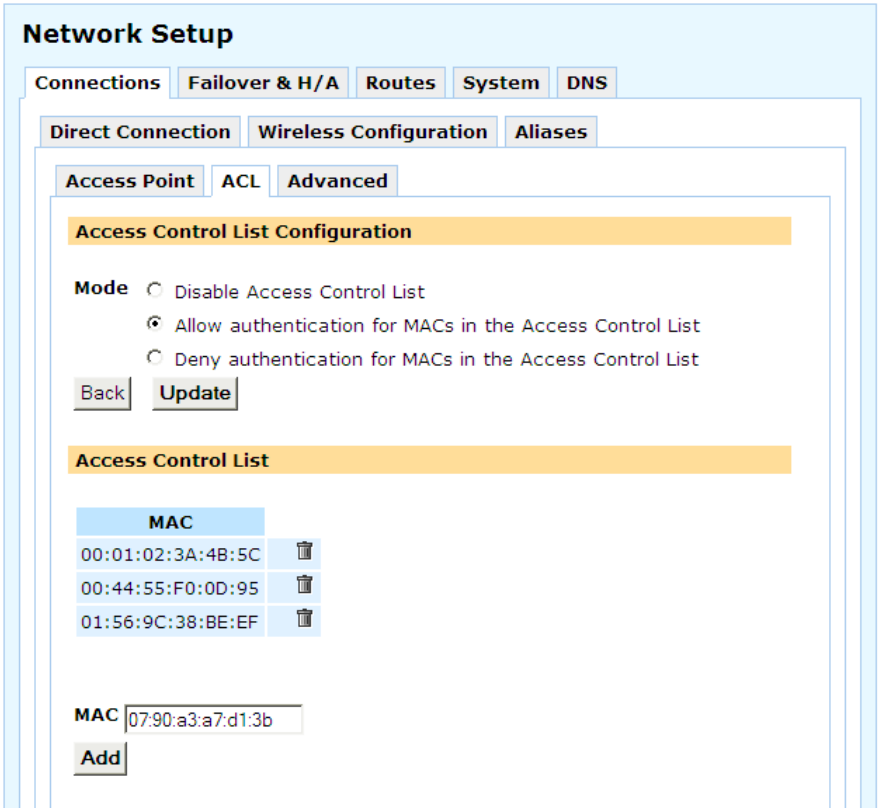
Alongside the **Wireless** network interface in the **Connections** menu, select **Direct Connection** from the **Change Type** pull down menu, or click **Edit** if you have previously configured wireless settings.



Click **Wireless Configuration**. Enter an appropriate **ESSID** and select a **Channel** for your wireless network. Enable **Bridge Between Clients** to allow wireless clients to intercommunicate, and there is generally no reason not to **Broadcast ESSID**. Take note of the **ESSID** and **Channel**, you need them to configure the wireless clients.

Select **WPA-PSK** as the **Security Method**, select **AES** for **WPA Encryption** if your wireless clients support it, otherwise select **TKIP**. Enter a **WPA Key** of 8 to 63 ASCII characters, or 64 hexadecimal characters. Take note of the **WPA Key** and **WPA Encryption** method, you need them to configure the wireless clients.

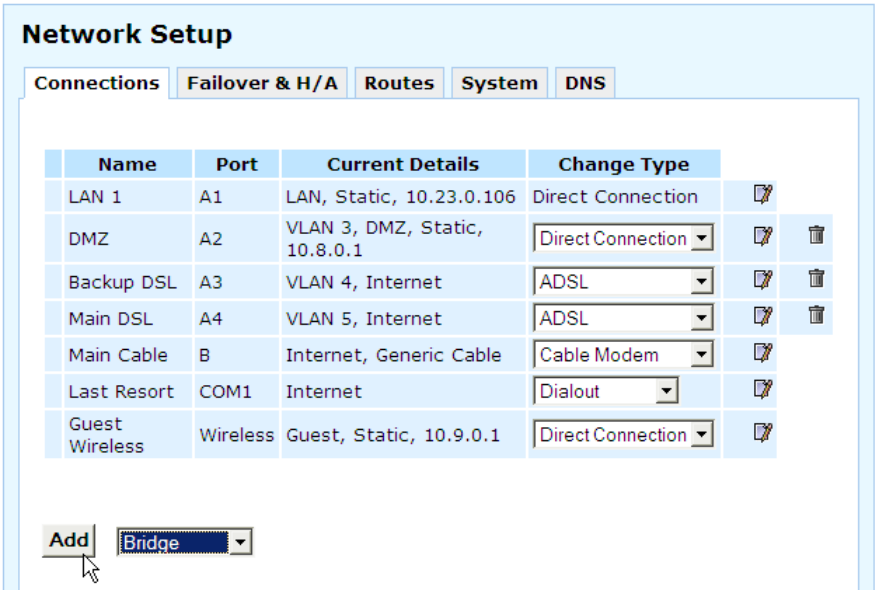
Click **Apply**. Click **ACL**.



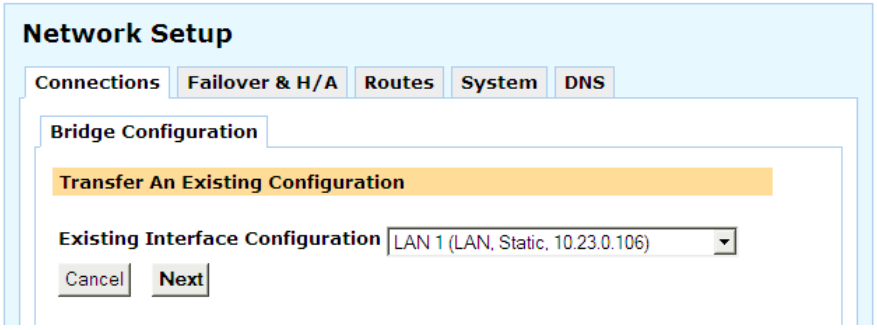
Select **Allow authentication for MACs in the Access Control List** and click **Apply**. **Add** the MAC address of each wireless client you wish to allow to connect.

Click **Advanced**. Ensure the **Region** has been set appropriately. You may also restrict the **Protocol** to **802.11b only** or **802.11g only** if you wish. Generally, the other settings should be left at their default values.

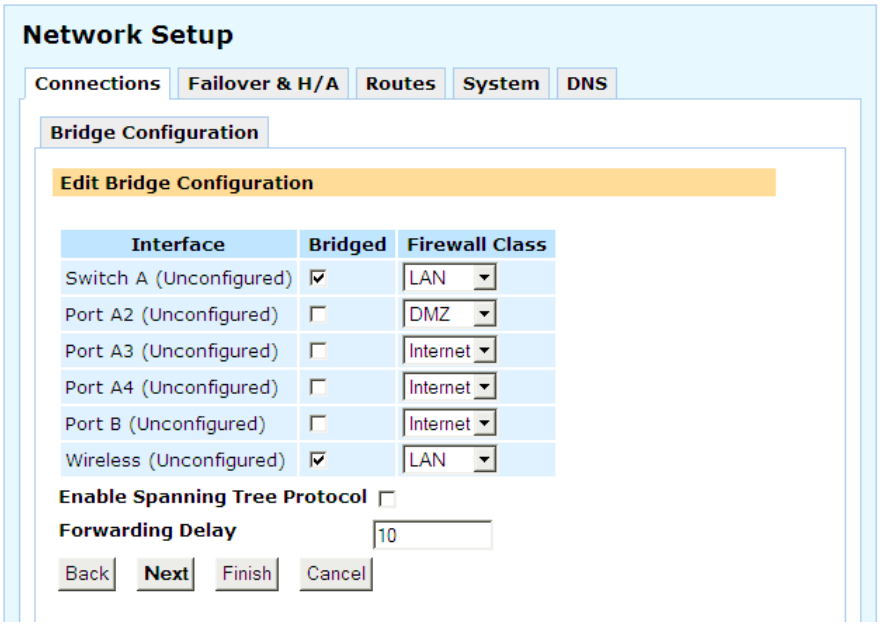
Click **Apply**. Click the **Connections** tab.



Under the main table, select **Bridge** and click **Add**.



Select your *wired* LAN connection from the **Existing Interface Configuration** pull down box. This is the address to share between the interfaces. Click **Next**.



Alongside the wireless interface, check **Bridged** and select **LAN** from the **Firewall Class** pull down menu. Click **Finish**.

Note

*If your **LAN** interface was previously configured to obtain an IP address automatically from a DHCP server, the SG unit now uses the MAC address of the wireless device when obtaining an IP address. You may have to update your DHCP server accordingly.*

Configure each wireless client with the **Channel**, **ESSID**, **WPA Key** and **WPA Encryption** method.

Bridging

The SG may be configured to bridge between network interfaces. When two or more network interfaces are bridged, the SG unit learns and keeps track of which hosts are reside on either side of the bridge, and automatically directs network traffic appropriately.

One advantage of bridging network interfaces is that hosts on either side of the bridge can communicate with hosts on the other side without having to specify a route to the other network via the SG unit.

Another advantage is that network traffic not usually routed by unbridged interface, such as broadcast packets, multicast packets, and any non-IP protocols such as IPv6, IPX or Appletalk pass over the bridge to their destination host.

Bridging network interfaces involves creating, then associating existing network interfaces with a **Bridge** interface.

Warning

You must trust all devices that are directly connected to bridged interfaces. This is because the firewall does not know which IP addresses for the bridged network belong on which interface. This means it is easy for a directly connected device to spoof an IP address. You can manually add Packet Filter *rules to prevent spoofing.*

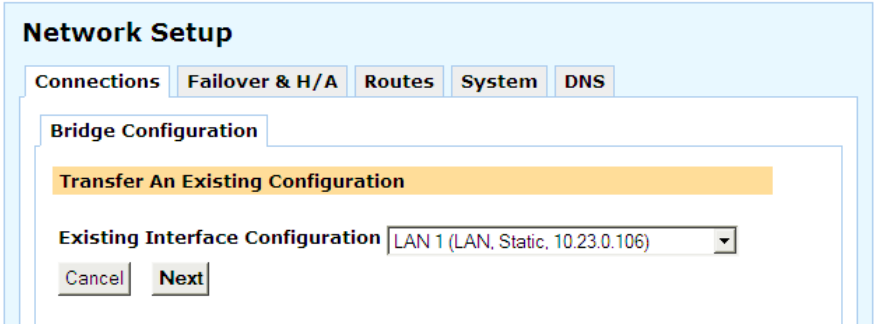
Furthermore, non-IP protocols are not restricted by the firewall. You should not bridge between interfaces with different firewall classes if you are using non-IP protocols.

Adding a bridge interface

From below the main **Connections** table, select **Bridge** from the pull down menu and click **Add**.

Once this bridge interface has been added, it appears on the **Network Setup** page under the **Connections** tab, along with the SG unit's other network interfaces.

When network interfaces are bridged, they all share a common configuration for the network connection. This means that a single IP address is used on all of the network interfaces.



If you wish to transfer the IP address settings of an existing network connection to the bridge interface, select it from the **Existing Interface Configuration** pull down menu. Click **Next**.

Note

As the SG unit automatically directs network traffic, hosts on either side do not need to specify this IP address as a gateway to the networks connected to the bridge.

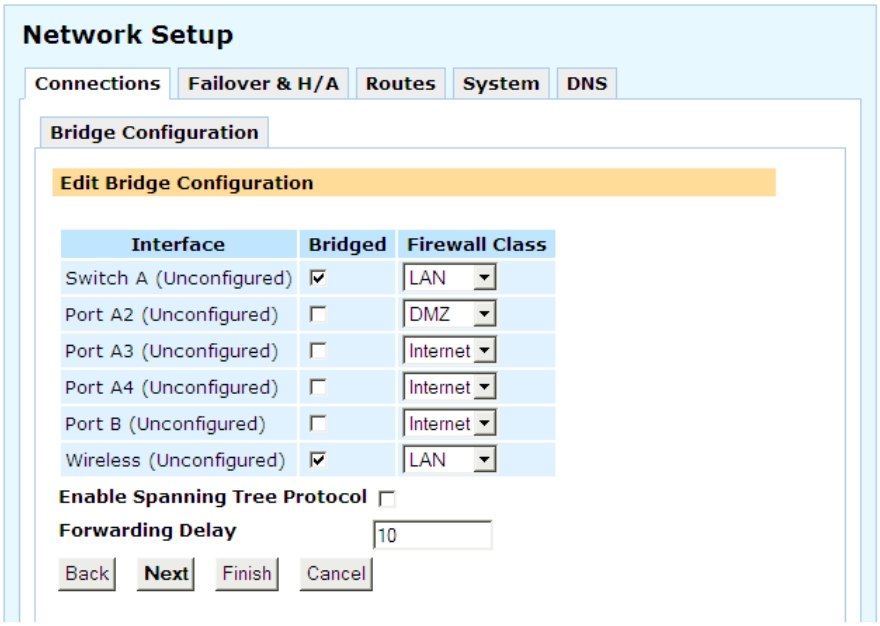
So in reality, it is not so important which IP address you choose to assign to the bridge interface; it is primarily used by hosts on either side of the bridge only to connect to the SG unit's web management console. Specific routes are still required to reach networks that are not being bridged.

Edit bridge configuration

For each network interface that you wish to bridge, select **Bridged**. Also ensure its **Firewall Class** is set appropriately; this setting is discussed in the *Direct Connection* section towards the beginning of this chapter.

Note

Bridging only supports ethernet and GRE network interfaces, and can only be configured as a Direct Connection. This means you cannot bridge a PPPoE connection.



You may want to **Enable Spanning Tree Protocol** if you have multiple bridges on your network. It allows the bridges to exchange information, helping elimate loops and find the optimal path for network traffic.

Forwarding Delay is the time in seconds between when the bridge interface comes online and when it begins forwarding packets. This usually only occurs when the unit first boots, or the bridge configuration is modified. This delay allows the SG unit's bridge to begin learning which hosts are connected to each of the bridge's interfaces, rather than blindly sending network traffic out all network interfaces.

Click **Next** to review or change IP address information for the bridge interface, otherwise click **Finish**.

Bridging across a VPN connection

Bridging across a VPN connection is useful for:

- Sending IPX/SPX over a VPN, something that is not supported by other VPN vendors
- Serving DHCP addresses to remote sites to ensure that they are under better control
- It allows users to make use of protocols that do not work well in a WAN environment (e.g. *netbios*)

A guide to bridging across an IPSec tunnel using GRE is provided in the section entitled *GRE over IPSec* in the *Virtual Private Networking* chapter.

VLANs

Note

VLANs are not *supported by the SG300.*

VLAN stands for virtual local area network. It is a method of creating multiple virtual network interfaces using a single physical network interface.

Packets in a VLAN are simply Ethernet packets that have an extra 4 bytes immediately after the Ethernet header. The format for these bytes is defined by the standard IEEE 802.1Q. Essentially, they provide for a VLAN ID and a priority. The VLAN ID is used to distinguish each VLAN. A packet containing a VLAN header is called a *tagged* packet.

When a packet is routed out the VLAN interface, the VLAN header is inserted and then the packet is sent out on the underlying physical interface. When a packet is received on the physical interface, it is checked for a VLAN header. If present, the router makes it appear as though the packet arrived on the corresponding VLAN interface.

Once added, VLAN interfaces can be configured through the **Network Setup** -> **Connections** table as if they were additional physical network interfaces.

Note

Since the addition and removal of the VLAN header are performed in software, any network device can support VLANs. Further, this means that VLANs should not be used for security unless you trust all the devices on the network segment.

A typical use of VLANs with the SG unit is to it to enforce access policies between ports on an external switch that supports port-based VLANs.

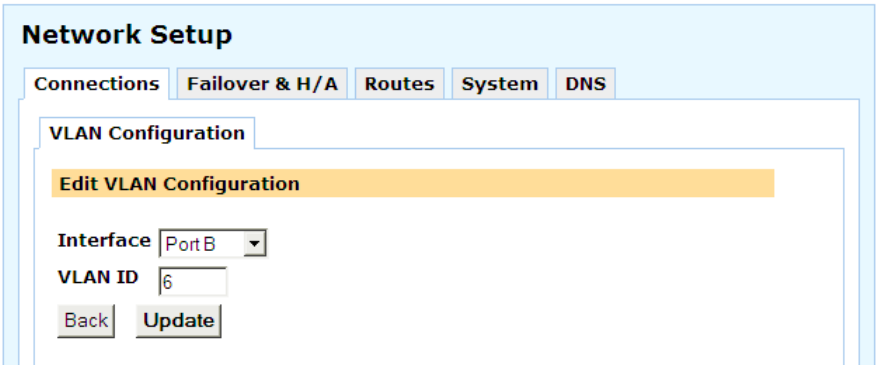
In this scenario, only the switch and other trusted devices should be directly connected to the LAN port of the SG unit. The SG unit and the switch are configured with a VLAN for each port or group of ports on the switch. The switch is configured to map packets between its ports and the VLANs. The SG unit can then be configured with firewall rules for the VLANs, and these rules are effectively applied to the corresponding ports on the switch.

Note

*Additionally, switch **A** on the SG560, SG565 and SG580 (but not the SG710 or SG710+) supports* port based VLANs*. One benefit of this feature is that you are able to assign individual functions to each of the ports on the switch, e.g. you might decide to use port **A2** to connect to a DMZ, and port **A3** as a second Internet connection. See the section entitled* Port Based VLANs *later in this chapter for details.*

Adding VLANs

On the **Network Setup** page under the **Connections** menu, select **VLAN** from the pull down menu and click **Add**.



- **Interface**: Select the network interface on which to add the VLAN
- **VLAN ID**: If this VLAN interface is to participate on an existing VLAN, the VLAN ID number must match the existing VLAN's ID
- **Port** / **Mode**: If this table is displayed, this interface has been enabled for port based VLANS; see the *Port Based VLANs* section later in this chapter

Click **Update**. You have now added a *tagged* VLAN interface that you may configure through the main **Network Setup** -> **Connections** menu as you would any other network interface.

Editing VLANs

Once a VLAN has been added, you may edit the settings you entered in *Adding VLANs* by clicking the **Edit** icon alongside the VLAN interface in the main **Network Setup** -> **Connections** table.

Removing VLANs

To remove a VLAN, click the **Delete** icon alongside the VLAN interface in the main **Network Setup** -> **Connections** table.

Port Based VLANs

Note

SG560, SG565 and SG580 only.

The SG560, SG565 and SG580 have a VLAN-capable switch built in. This gives you the flexibility to either use it as a simple switch that allows access between all ports (this is the default), or use port based VLANs to control access between each individual port in the switch.

This port based VLAN configuration makes it possible to assign each of the four ports its own subnet address, declare it to be a LAN, WAN or DMZ independent of the other ports and generally treat it as if it was a completely separate physical port.

The SG unit may also participate on an existing VLAN. When you add a VLAN interface to connect to the existing VLAN, you may associate it with one or more of the SG unit's ports.

Tagged and untagged VLANs

When using port based VLANs, it is important to understand the differences between tagged and untagged VLANs.

Tagged VLAN interfaces add a VLAN header (see the VLAN *Overview* section earlier in this chapter) to outgoing network packets, and only accept incoming network packets that contain an appropriate VLAN header. Untagged VLAN interfaces do *not* add a VLAN header to outgoing network packets, and do *not* accept incoming packets that contains a VLAN header.

A port may be a member of either a single untagged VLAN, or one or more tagged VLANs. A port may *not* be a member of both tagged and untagged VLANs.

Once switch **A** has had port based VLANs enabled, ports that have not been explicitly assigned to one or more VLANs are assigned to the default VLAN. The default VLAN is untagged.

Typically, a tagged VLAN interface is used when you want to join an existing VLAN on the network, and an untagged VLAN interface is used when you are using the port based VLAN feature to isolate the ports so that you can configure each of them individually.

Limitations of port based VLANs

There are few further limitations to keep in mind when using port based VLANs:

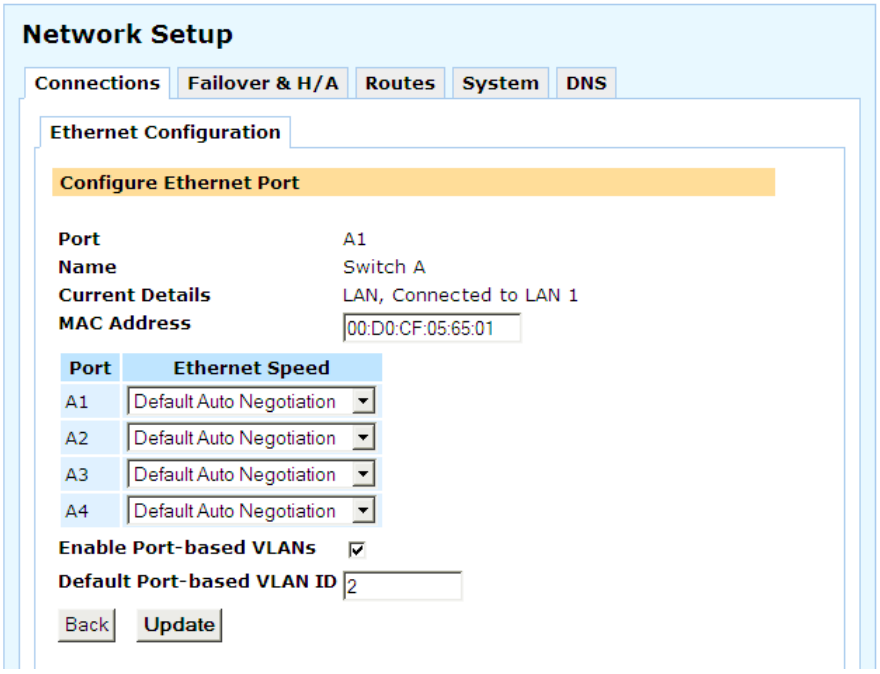
- The total bandwidth from the switch into the CPU is 100Mbits/s, which is shared between the 4 ports. This may limit the bandwidth available to a single port when perform general routing, packet filtering and other activities.
- Port based VLANs can only be enabled if there are less than 16 total VLANs.
- Switch **A** can only have one default VLAN, and any ports that are not explicity assigned to another VLAN are automatically placed on the default VLAN. The default VLAN is untagged.
- You cannot add tagged VLANs to port **A1**; it is a member of the default VLAN only.

Enabling port based VLANs

Note

*If you previously selected **1 LAN Port, 3 Isolated Ports** in the **Switch Configuration** step of the Quick Setup Wizard, port based VLANs are already enabled.*

Select **Network Setup** from the **Networking** menu. Next to the port based VLAN capable interface (**Switch A** on the SG560, SG565 and SG580), click the **Edit** icon then the **Ethernet Configuration** tab.



The following settings pertain to port based VLANs:

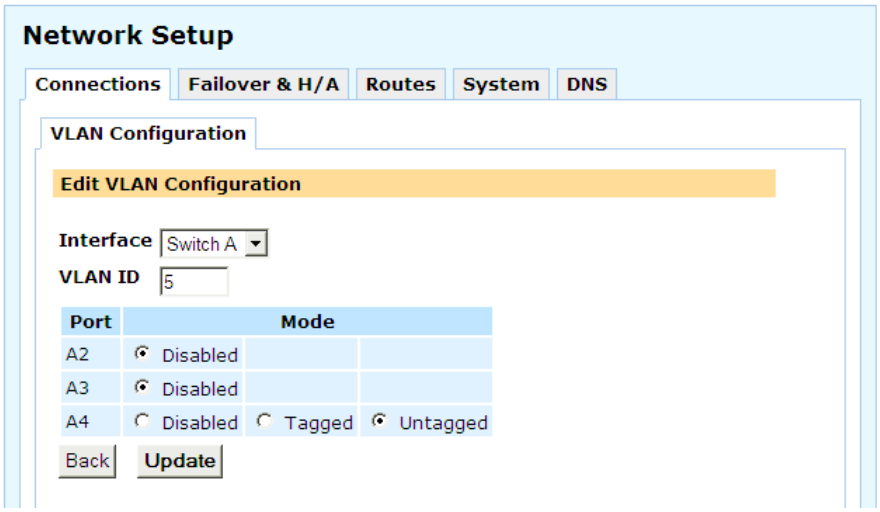
- **Enable port based VLANs:** Check to enable port based VLANs.
- **Default port based VLAN ID:** As the default VLAN is always untagged, typically you only need to change this from the default setting of 2 if you want another port to participate on an existing tagged VLAN with the ID of 2.

Adding port based VLANs

Note

*If you previously selected **1 LAN Port, 3 Isolated Ports** in the **Switch Configuration** step of the Quick Setup Wizard, a single isolated VLAN for each port has already been added.*

Select **Network Setup** from the **Networking** menu. Under the **Connection** table, select **VLAN** and click **Add**.



The following settings are displayed:

- **Interface:** The port based VLAN capable interface on which to add the VLAN.

- **VLAN ID:** If you are adding a VLAN interface to participate on an existing VLAN, enter its ID number here. Otherwise enter the next available VLAN ID; if the **Default port based VLAN ID** has been left at its default setting of 2, **Port A2** uses VLAN ID 3, **Port A3** uses VLAN ID 4, and so on.

  Note

  Some Cisco equipment uses tagged VLAN 1 for its own purposes. We therefore recommend setting the default VLAN ID to 2 or greater for tagged VLANs, unless you intend for the SG unit and Cisco equipment to interact over tagged VLAN 1.

- **Mode:** This is where you associate one or more of switch **A**'s ports with this VLAN interface. Select **Disabled** for the ports to exclude from this VLAN. If you are configuring a port or ports to participate on an existing tagged VLAN, set them **Tagged**. Otherwise, to isolate a single port so that it may be configured individually, set the port **Untagged**.

Refer to the section entitled *Tagged and untagged VLANs* earlier in this chapter for further discussion of these settings.

Click **Update**. This VLAN interface now appears in the **Connections** table, and you may configure it as you would any other network interface.

Editing port based VLANs

Once a VLAN has been added, you may edit the settings you entered in *Adding port based VLANs* by clicking its **Edit** icon in the main **Network Setup -> Connections** table.

Removing port based VLANs

To remove a VLAN, click its **Delete** icon in the main **Network Setup -> Connections** table.

GRE Tunnels

The GRE configuration of the SG unit allows you to build GRE tunnels to other devices that support the *Generic Routing Encapsulating* protocol. You can build GRE tunnels to other SG units that support GRE, or to other devices such as Cisco equipment.

GRE tunnels are useful for redistributing IPv6 or broadcast and multicast traffic across a VPN connection. It is also useful for carrying unsupported protocols such as IPX or Appletalk between remote IP networks.

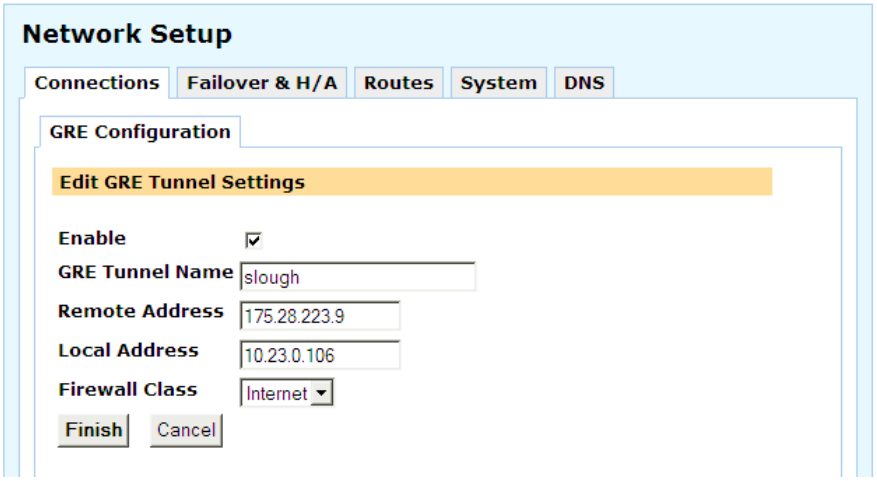
Warning

GRE tunnels are not secure unless they are run over another secure protocol. Using a GRE tunnel that runs over the Internet, it is possible for an attacker to put packets onto your network. If you want a tunneling mechanism to securely connect to networks, then you should use IPSec, or tunnel GRE over either IPSec or PPTP tunnels.

An example setup that describes using GRE to bridge a network over an IPSec tunnel is described in GRE over IPSec*.*

Adding a GRE interface

Under the **Network Setup -> Connections** table, select **GRE Tunnel** and click **Add**.



Ensure **Enable** is checked and enter a descriptive **GRE Tunnel Name** for this tunnel.

Enter the address of the remote GRE endpoint in **Remote Address**, e.g. the Internet IP address of a remote SG unit.

Enter the address of the local GRE endpoint in **Local Address**. This is typically a free address on your main LAN. If your LAN connection has an alias address, it may also be a free address on the alias network.

Select a **Firewall Class** for the GRE interface, this setting is discussed in the *Direct Connection* section towards the beginning of this chapter.

Click **Finish**. The GRE interface now appears in the main **Network Setup** table.

GRE over IPSec

The basic steps to set up GRE over IPSec are:

1. Use the same network for the primary IP addresses of the LAN interfaces at both ends of the tunnel.
2. Assign unused alias IP addresses to the LAN interfaces at both ends of the tunnel.
3. Create an IPSec tunnel between the alias IP addresses.
4. Create a GRE tunnel between the alias IP addresses.
5. Create bridges between the LAN interfaces and the GRE tunnel.

6. Modify the firewall.

In this example we use a dummy alias network of 10.254.0.0 / 255.255.0.0 to bridge two example local networks, one at Brisbane and one at Slough. These steps must be repeated for either end of the tunnel.

Note that the two locations are using the same subnet.

SG unit in Brisbane

Internet address:	203.23.45.6
LAN address:	192.168.1.1
LAN alias:	10.254.0.1
LAN:	192.168.1.0 / 24

SG unit in Slough

Internet address:	195.45.67.8
LAN address:	192.168.1.2
LAN alias:	10.254.0.2
LAN:	192.168.1.0 / 24

Add the LAN connection to a bridge, as described in the section entitled *Bridging* earlier in this chapter.

Give the LAN interface bridge a secondary address that is part of the network we want bridged across the tunnel. Adding an alias is described in *Aliases* in the section entitled *Direction Connection* earlier in this chapter. In this example, the Brisbane end uses an alias address of 10.254.0.1, the Slough end uses and alias address of 10.254.0.2.

Ensure the alias address is *not* part of the network to bridge across the tunnel (in this example, it mustn't be part of 192.168.0.0 / 24), and *not* on the same network as any of the SG unit's other interfaces.

Note

The alias IP addresses are essentially dummy addresses and can be anything that does not conflict with your existing network infrastructure.

Create an IPSec tunnel between Brisbane and Slough. Select **IPSec** from the **VPN** section of the main menu and click **New**. For a complete overview of all available options when setting up an IPSec tunnel, refer to the *IPSec* section earlier in this chapter.

Take note of the following important settings:

Set the **local party** as a **single network behind this appliance**. Set the **remote party** as **single network behind a gateway**.

For the Slough end's **Phase 2 Settings**, specify the **Local Network** as *10.254.0.1* / *255.255.255.255* and the **Remote Network** as *10.254.0.2* / *255.255.255.255*. For the Brisbane end's **Phase 2 Settings**, specify the **Local Network** as *10.254.0.2* / *255.255.255.255* and the **Remote Network** as *10.254.0.1* / *255.255.255.255*. Note the 32 bit netmasks (255.255.255.255) being used.

Create the GRE tunnel. Under the main **Network Setup** table, select **GRE Tunnel** and click **Add**. For the Slough end, enter:

GRE Tunnel Name:	*to_bris*
Remote Address:	*10.254.0.2*
Local Address:	*10.254.0.1*
Firewall Class:	*LAN*

For the Brisbane end, enter:

GRE Tunnel Name:	*to_slough*
Remote External Address:	*10.254.0.1*
Local External Address:	*10.254.0.2*
Firewall Class:	*LAN*

Click **Finish** to add the interface. **Edit** the bridge interface that you added at the beginning of these steps. Check **Bridged** for the GRE interface you have just added, and select a **Firewall Class** of **LAN**. Click **Finish**.

At the Slough end, click **Packet Filtering**, the **Custom Firewall Rules** tab and add this custom firewall rule:

```
iptables -I OUTPUT ! -o ipsec+ -d 10.254.0.2 -j DROP
```

Click **Update**.

At the Brisbane end, click **Packet Filtering**, the **Custom Firewall Rules** tab and add this custom firewall rule:

```
iptables -I OUTPUT ! -o ipsec+ -d 10.254.0.1 -j DROP
```

Click **Update**.

GRE troubleshooting

- **Symptom:** Cannot ping a host on the other side of the GRE tunnel.

  Ensure that there is a route set up on the GRE tunnel to the remote network.

  Ensure that there is a route on the remote GRE endpoint to the network at this end of the GRE tunnel.

  Check that there is a GRE interface created on the device. To do this, go into *Advanced Networking* and scroll to the bottom. There should be an interface called **gre***X* created. **gre***X* is the same as the **Interface Name** specified in the table of current GRE tunnels.

  Also ensure that the required routes have been set up on the GRE interface. This might not occur if you have the same route specified on different GRE tunnels, or on different network interfaces.

  Ensure that the remote GRE endpoint is reacheable. Do this by using the ping utility on the *Advanced Networking* page.

- **Symptom:** Cannot ping the remote GRE end point.

  Ensure that the remote GRE end point responds to pings. Note that by default no packets are routed across the GRE tunnel unless there is a route setup on the GRE tunnel.

Routes

To configure the SG unit's advanced routing features, click the **Routes** tab on the **Network Setup** page.

Static routes

Here you may add additional static routes for the SG unit. These routes are additional to those created automatically by the SG unit configuration scripts.

Click **New** to add a static route. **Target Address** and **Subnet mask** identify the destination network or host. You may also specify an **Interface** out which the network traffic should be routed, a **Gateway Address** through which the network traffic should be routed, and a **Metric** for this route.

Route management

Note

Route management does not have full GUI configuration support. We recommend that only advanced users familiar with the Zebra routing daemon and/or the RIP, BGP or OSPF routing protocol attempt configuration of this feature.

Advanced users may configure the SG unit to automatically manage its routing tables, exchanging routes with other routers using RIP, BGP or OSPF protocol.

Check **Enable route management**, select the desired **Protocol** and click **Update**.

The routing manager must now be configured manually by editing the appropriate configuration files. Select **Advanced** from the **System** menu and select the **Configuration Files** tab. Check **zebra.conf** and ***protocol*d.conf** configuration file (e.g. **ripd.conf**) and click **Modify**.

A relatively trivial example for each protocol is given below. You should not rely on these guides to configure route management for your network, please refer to the Zebra web site (http://www.zebra.org) for comprehensive documentation.

RIP

Ensure you have enabled **RIP(v1, v2)** under **Route Management**, then open **zebra.conf** and **ripd.conf** for editing as described in the *Route management* section.

Note

! *and # are comment characters. If the first character of the word is one of the comment characters then from the rest of the line forward is ignored as a comment:*

! password zebra

If a comment character is not the first character of the word, it's a normal character. In the example below, ***!*** *is not regarded as a comment and the password is set to* ***zebra!password****:*

password zebra!password

*In these examples,**!** denotes a descriptive comment, and # indicates a configuration line that is currently commented out, that you may want to uncomment depending on your network setup.*

In **zebra.conf**, enter:

```
! Uncomment and set telnet/vty passwords to enable telnet
access on port 2601
#password changeme
#enable password changeme

! Uncomment no multicast if you dont wan’t to accept or send
multicast rip packets for the specified interface
#interface eth0
#no multicast
#interface eth2
#no multicast
```

In **ripd.conf**, enter:

```
! Uncomment and set telnet/vty passwords to enable telnet
access on port 2602
#password changeme
#enable password changeme

! RIP version 2 authentication
#interface eth0
#ip rip authentication mode text
#ip rip authentication string snapgear

! Enable the RIP routing process
router rip
! Define interfaces which exchange RIP messages over
network eth0
```

```
#network eth2

! Define neighbor routers to exchange RIP with if disabling
multicast above in zebra.conf, or neighbors don't have
multicast enabled

#neighbor 192.168.45.238

#neighbor 192.168.45.231

! Redistribute routing information for interfaces with RIP
disabled

redistribute connected

! Redistribute routing information from static route entries

redistribute static

! Redistribute routing information from kernel route entries
e.g. IPSec

redistribute kernel
```

Note

RIP version 2 is used by default.

The above files configure the device to listen for and send multicast RIP messages on the eth0 (LAN port) interface. You can see the above example has commented out additional interfaces which to exchange RIP messages over and optional neighbors routers to exchange RIP messages with if these neighbours can't accept multicast packets. There is also an example for setting up RIP version 2 authentication. Uncomment and configure as required.

Restart route management to enable the updated configuration – uncheck **Enable route management**, click **Update**, check **Enable route management** and click **Update**.

If you prefer, you can uncomment the **password** and **enable password** lines, and then telnet to the relevant ports to configure Zebra and/or ripd via the command line. The command line interface is very similar to the Cisco IOS interface. If you are familiar with this, you may prefer to configure using this method.

OSPF

Note

This example is adapted from the LARTC (Linux Advanced Routing & Traffic Control) dynamic routing howto, available from: http://lartc.org/howto/

LARTC is an invaluable resource for those wanting to learn about and take advantage the advanced routing capabilities of Linux systems.

OSPF stands for Open Shortest Path First, and some of its principal features are:

- Networks are grouped by *areas*, which are interconnected by a *backbone area* which will be designated as *area 0*. All traffic goes through area 0, and all the routers in area 0 have routing information about all the other areas.

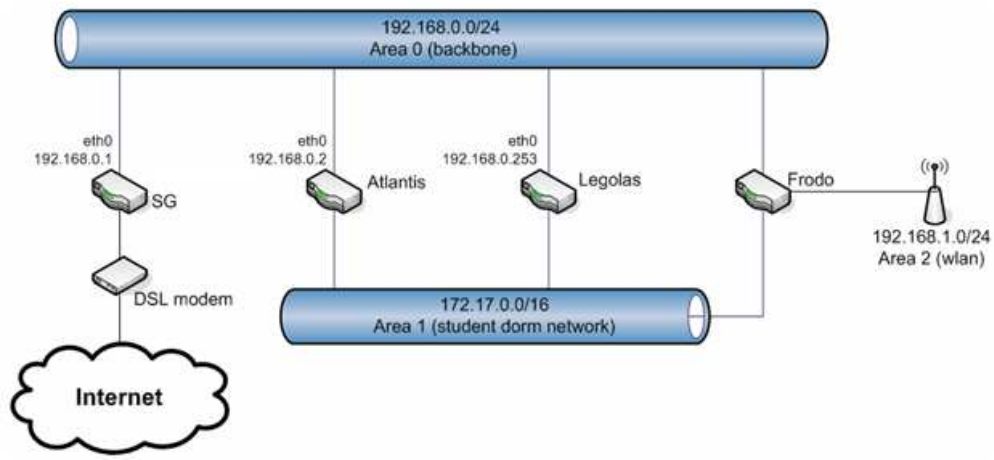
- Routes are propagated very fast, compared with RIP, for example.

- OSPF uses multicasting instead of broadcasting, so it doesn't flood other hosts with routing information that may not be of interest for them, thus reducing network overhead. Also, *Internal Routers* (those which only have interfaces in one area) don't have routing information about other areas. Routers with interfaces in more than one area are called *Area Border Routers*, and hold topological information about the areas they are connected to.

- OSPF is based on Dijkstra's Shortest Path First algorithm, which is CPU intensive compared to other routing algorithms. But really is not that bad, since the Shortest Path is only calculated for each area, also for small to medium sized networks this won't be an issue, and you won't even notice.

- OSPF counts with the special characteristics of networks and interfaces, such as bandwidth, link failures, and monetary cost.

In this example we set up route management using OSPF for the network topology described by the following diagram.



The SG is configured to exchange routes with the routers named *Atlantis*, *Legolas* and *Frodo*.

Ensure you have enabled **OSPF** under **Route Management**, then open **zebra.conf** and **ospfd.conf** for editing as described in the *Route management* section.

In **zebra.conf**, enter:

```
hostname sg

! Uncomment and set telnet/vty passwords to enable telnet
access on port 2602
#password changeme
#enable password changeme


# Enable multicast for OSPF
interface eth1
multicast


! Example static default route for Internet connection
#ip route 0.0.0.0/0 212.170.21.129
```

In **ospfd.conf**, enter:

```
hostname sg
```

```
! Uncomment and set telnet/vty passwords to enable telnet
access on port 2604
#password changeme
#enable password changeme

! Instruct ospfd about our network topology
router ospf
  network 192.168.0.0/24 area 0
  network 172.17.0.0/16 area 1
```

Restart route management to enable the updated configuration – uncheck **Enable route management**, click **Update**, check **Enable route management** and click **Update**.

Restart route management to enable the updated configuration – uncheck **Enable route management**, click **Update**, check **Enable route management** and click **Update**.

If you prefer, you can uncomment the **password** and **enable password** lines, and then telnet to the relevant ports to configure Zebra and/or ospfd via the command line. The command line interface is very similar to the Cisco IOS interface. If you are familiar with this, you may prefer to configure using this method.

BGP

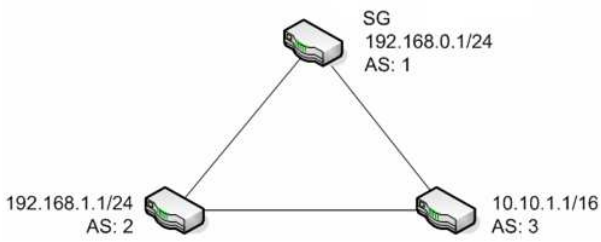
Note

This example is adapted from the LARTC (Linux Advanced Routing & Traffic Control) dynamic routing howto, available from: http://lartc.org/howto/

LARTC is an invaluable resource for those wanting to learn about and take advantage the advanced routing capabilities of Linux systems.

The Border Gateway Protocol (BGP) allows the distribution of reachability information, i.e. routing tables, to other BGP enabled nodes. It can either be used as EGP or IGP, in EGP mode each node must have its own Autonomous System (AS) number. BGP supports Classless Inter Domain Routing (CIDR) and route aggregation (merge multiple routes into one).

The following network map is used for this example. AS 2 and 3 have more neighbors but we only need to configure 2 and 3 as our neighbor.



Note

The AS numbers used in this example are reserved, please get your own AS from RIPE if you set up official peerings.

Ensure you have enabled **BGP** under **Route Management**, then open **zebra.conf** and **bgpd.conf** for editing as described in the *Route management* section.

In **zebra.conf**, enter:

```
hostname sg

! Uncomment and set telnet/vty passwords to enable telnet
access on port 2602
#password changeme
#enable password changeme
```

In **bgpd.conf**, enter:

```
hostname sg

! Uncomment and set telnet/vty passwords to enable telnet
access on port 2605
#password changeme
#enable password changeme


! Access list, used to limit the redistribution to private
networks (RFC 1918)
access-list local_nets permit 192.168.0.0/16
access-list local_nets permit 172.16.0.0/12
access-list local_nets permit 10.0.0.0/8
```

```
access-list local_nets deny any


! Our AS number
router bgp 1
   ! Our IP address
   bgp router-id 192.168.0.1
   ! Announce our own network to other neighbors
   network 192.168.0.0/24
   ! Advertise all connected routes (directly attached interfaces)
   redistribute connected
   ! Advertise kernel routes (manually inserted routes, IPSec)
   redistribute kernel
   ! Every 'router bgp' block contains a list of neighbors to
   which the router is connected:
   neighbor 192.168.1.1 remote-as 2
   neighbor 192.168.1.1 distribute-list local_nets in
   neighbor 10.10.1.1   remote-as 3
   neighbor 10.10.1.1   distribute-list local_nets in
```

Restart route management to enable the updated configuration – uncheck **Enable route management**, click **Update**, check **Enable route management** and click **Update**.

If you prefer, you can uncomment the **password** and **enable password** lines, and then telnet to the relevant ports to configure Zebra and/or ospfd via the command line. The command line interface is very similar to the Cisco IOS interface. If you are familiar with this, you may prefer to configure using this method.

System

To configure the SG unit's network system settings, click the **System** tab on the **Network Setup** page. These settings control the SG unit's identity on the network.

Hostname

The **Hostname** is a descriptive name for the SG unit on the network. It is also used as the SNMP *sysName* field. By default, this is set to the model name of your SG unit, e.g. *SG710*.

If network shares or printers are being shared, this is the computer name that is displayed when browsing the network from a Windows PC *(SG565 only)*.

Workgroup/domain

Note

SG565 only.

The **Workgroup/Domain** is the Windows workgroup or domain with which to share printers or network shares. These shared resources are not visible to machines on the LAN that are not members of this workgroup or domain.

Administrative contact

You may enter the email address of the local administrator of the SG unit for use as the SNMP *sysContact* field.

Device location

You may also enter a short description of the physical location of the SG unit for use as the SNMP *sysLocation* field.

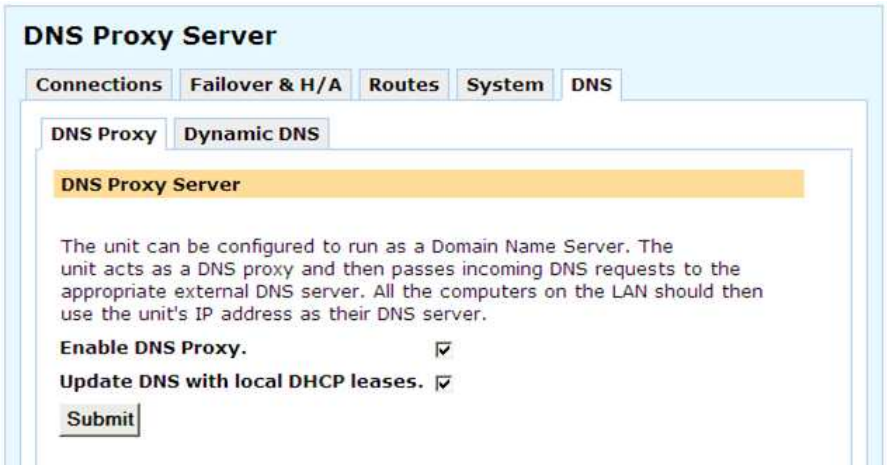
DNS

To configure the SG unit's DNS settings, click the **DNS** tab on the **Network Setup** page. These settings control the SG unit's network name services.

DNS proxy

The SG unit can also be configured to run a domain name server (DNS) proxy. The SG unit passes incoming DNS requests from internal clients to an external DNS server, and forwards the reply back to the internal client.

If this is enabled, all the computers on the LAN can specify the IP address of the SG unit as their DNS server.


DNS Proxy Server
Connections
Failover & H/A
Routes
System
DNS
DNS Proxy
Dynamic DNS
DNS Proxy Server
The unit can be configured to run as a Domain Name Server. The unit acts as a DNS proxy and then passes incoming DNS requests to the appropriate external DNS server. All the computers on the LAN should then use the unit's IP address as their DNS server.
Enable DNS Proxy.
Update DNS with local DHCP leases.
Submit

Check **Enable DNS proxy** to enable this feature. If you are using the SG unit's DHCP server, you may also check **Update DNS with local DHCP leases**. This allows the SG unit's DNS proxy to look up the names of devices that have requested IP address addresses.

Dynamic DNS

A dynamic DNS service is useful when you don't have a static Internet IP address, but need to remain contactable by hosts on the Internet. Dynamic DNS service providers such as TZO.com and dyndns.org can register an Internet domain name that points to your Internet IP address no matter how often it changes.

Whenever its Internet IP address changes, the SG unit alerts the dynamic DNS service provider and the domain name records are updated appropriately.

First, create an account with the dynamic DNS service provider of your choice, then select this service provider from the **Service** pull down menu and click **New**.

Select the **Port** that you want associated with your newly created DNS name. You may select **Default Gateway Interface** to have the SG unit use the external port of your Internet connection.

Enter the details provided by your dynamic DNS service provider and click **Apply** to enable.

DHCP Server

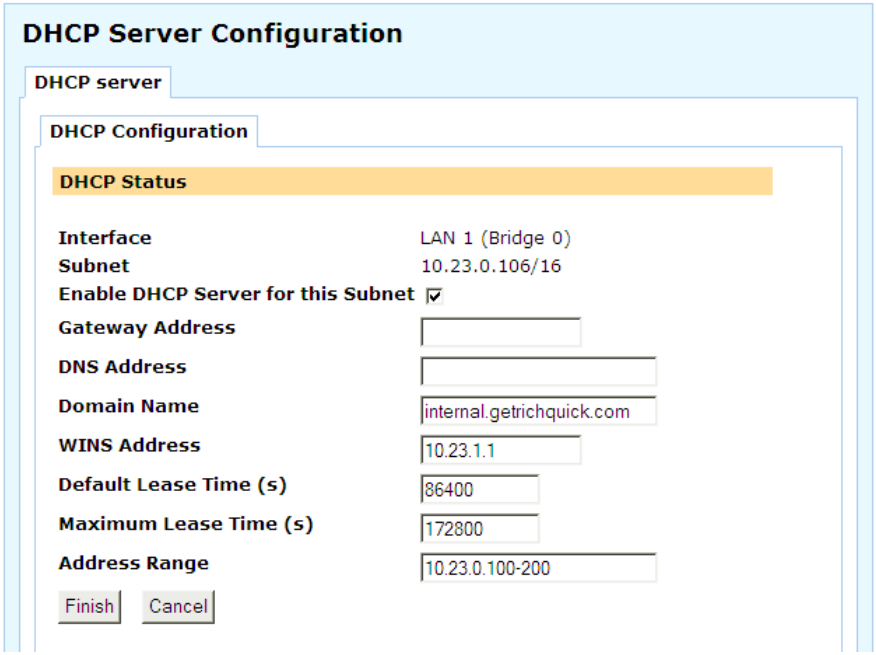
Note

To configure your SG unit as a DHCP server, you must set a static IP address and netmask on the network interface on which you want the DHCP server to run; see the Direct Connection *section of the chapter entitled* Network Connections*.*

To begin configuring the SG unit's DHCP server, select **DHCP Server** from the **Network Setup** section of the web management console's main menu.

DHCP configuration

Click the **Edit** icon next to the network interface on which you wish to edit or enable a DHCP server.



To configure the DHCP server, follow these instructions.

- Check the **Enable DHCP Server for this Subnet** checkbox.
- Enter the **Gateway Address** to issue the DHCP clients. If this field is left blank, the SG unit's IP address is used.

- Enter the **DNS Address** to issue the DHCP clients. If this field is left blank, the SG unit's IP address is used. Leave this field blank for automatic DNS server assignment. If your SG unit is configured for DNS masquerading, you should either leave this field blank, or enter the IP address of the LAN port of the SG unit.

- Optionally enter a **Domain Name** suffix to issue DHCP clients.

- Optionally enter IP address of the WINS server to be distributed to DHCP clients in the **WINS Address** field.

- Enter the **Default Lease Time** and **Maximum Lease Time** in seconds. The lease time is the time that a dynamically assigned IP address is valid before the client must re-request it.

- Enter the IP address or range of IP addresses (see the appendix entitled *IP Address Ranges*) to be issued to DHCP clients in the **Address Range** field.

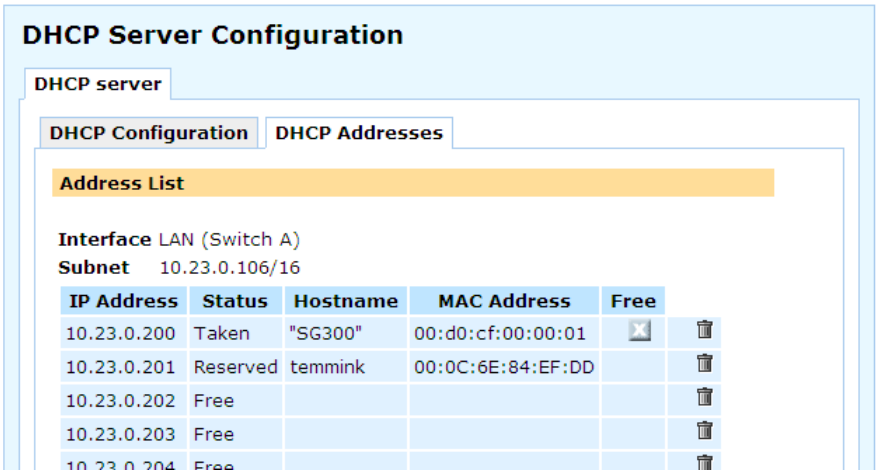
Click **Finish**.

DHCP addresses

To view the status of the IP address the DHCP server is configured to distribute, click the **Edit** icon next to the appropriate network interface, then click the **DHCP Addresses** tab.

Address list

For each **IP Address** that the DHCP server is managing, the **Status**, **Hostname**, **MAC Address** is displayed.



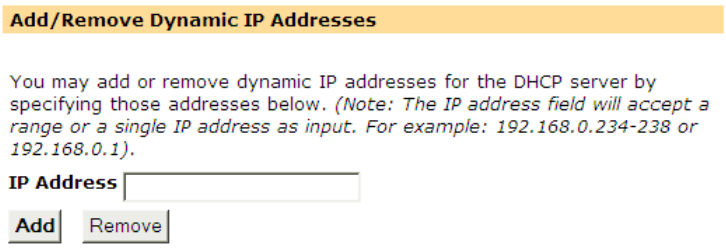
There is an icon to **Delete** the address from the list of addresses to manage. You may also **Free** addresses that have been leased by hosts on your network, this causes the lease to expire immediately, leaving the address available for the next host that requests IP configuration.

The **Status** field displays one of three states:

- **Reserved:** the address is reserved for the particular host defined by hostname and MAC address
- **Free:** the address is available to be handed out to any DHCP client host
- **Taken:** the address has been issued to a host

Adding and removing addresses

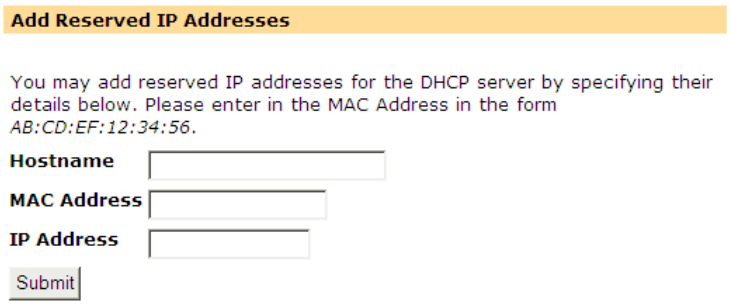
Under **Add/Remove Dynamic IP Addresses**, enter the IP address or IP address range and click **Add** or **Remove**.


Add/Remove Dynamic IP Addresses
You may add or remove dynamic IP addresses for the DHCP server by specifying those addresses below. (Note: The IP address field will accept a range or a single IP address as input. For example: 192.168.0.234-238 or 192.168.0.1).
IP Address
Add
Remove

To remove an address, you may also click its **Delete** icon under the **Address List**.

Reserving IP addresses

You may also reserve IP addresses for particular hosts, identifying them by hostname and MAC address.


Add Reserved IP Addresses
You may add reserved IP addresses for the DHCP server by specifying their details below. Please enter in the MAC Address in the form AB:CD:EF:12:34:56.
Hostname
MAC Address
IP Address
Submit

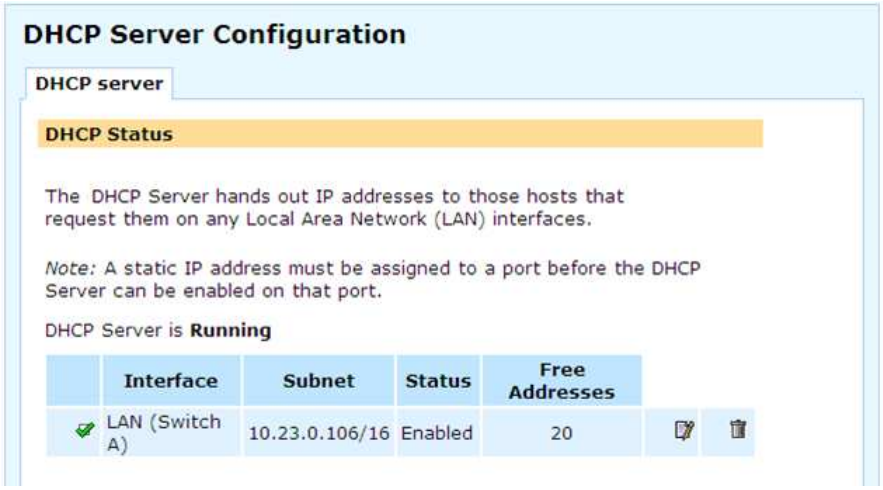
To reserve an IP address for a certain host, enter the following in the **Add reserved IP address** section.

- Enter the **Hostname** of the DHCP client.
- Enter the **MAC address** of the DHCP client.
- Enter the reserved **IP address** for the DHCP client.

Click **Submit**.

DHCP status

This main DHCP server page displays the status for each interface on which the DHCP server is running. There are **Edit**, **Delete** and **Enable/Disable** icons displayed for each Interface.


DHCP Server Configuration
DHCP server
DHCP Status
The DHCP Server hands out IP addresses to those hosts that request them on any Local Area Network (LAN) interfaces.
Note: A static IP address must be assigned to a port before the DHCP Server can be enabled on that port.
DHCP Server is Running
Interface
Subnet
Status
Free Addresses
LAN (Switch A)
10.23.0.106/16
Enabled
20

The **Subnet** is the network on which DHCP server is handing out addresses. **Free Addresses** displays the number of remaining available IP addresses that can be distributed. You may need to increase the number of IP addresses to hand out if this value is 0.

DHCP Proxy

The DHCP proxy allows the SG unit to forward DHCP requests from the LAN to an external server for resolution. This allows both static and dynamic addresses to be given out on the LAN just as running a DHCP server would.

To enable this feature, specify the server which is to receive the forwarded requests in **Relay Host**. This server must also be configured to know and accept requests from the SG unit's LAN. Then check **Enable DHCP Relay** and click **Apply**.

Web Cache

Note

SG565, SG575, SG635 and SG rack mount appliances only.

Web browsers running on PCs on your LAN can use the SG unit's proxy-cache server to reduce Internet access time and bandwidth consumption.

A proxy-cache server implements Internet object caching. This is a way to store requested Internet objects (i.e., data available via HTTP, FTP, and other protocols) on a server closer to the user's network than on the remote site. Typically the proxy-cache server eliminates the need to re-download Internet objects over the available Internet connection when several users attempt to access the same web site simultaneously. The web site's contents are available in the cache (server memory or disk) and quickly accessible over the LAN rather than the slower Internet link.

The SG unit's web cache keeps objects cached in memory and on a LAN network share, caches Internet name (DNS) lookups and implements negative caching of failed requests.

Using the lightweight Internet Cache Protocol, multiple web caches can be arranged in a hierarchy or mesh. This allows web cache peers to pull objects from each other's caches, further improving the performance of web access for an organisation with multiple Internet gateway.

The SG unit's web cache may also be configured to pass off web transation requests or responses to a third-party ICAP server for processing, using its *ICAP client*. This is typically used to integrate a third-party virus scanning, content filtering or complete CSM solution, such as WebWasher (http://www.webwasher.com).

Enabling the web cache

Select **Web cache** under **Network Setup**. Check **Enable** to enable the web cache.

Selecting a cache size

Select the amount of memory (RAM) on the SG unit to be reserved for caching Internet objects. The maximum amount of memory you can safely reserve depends on what other services the SG unit has running, such as VPN or a DHCP server.

If you are using a **Network Share** or **Local Storage** (recommended, see below), it is generally best to set this to **8 Megabytes**.

Otherwise, start with a small cache (**8 Megabytes** or **16 Megabytes**) and gradually increase it until you find a safe upper limit where the SG unit can still operate reliably.

Storage

The web cache is capable of utilizing a storage device attached via the USB port, or a network share to provide backing store for the cache. Using this greatly increases the effectiveness of the cache.

Local storage

Note

Network Storage *and* ***Local Storage*** *cannot be used at the same time. Enabling one will automatically disable the other.*

Attach a USB storage device, click **Storage** then **Local Storage**.

Enter a **Cache size** in MB. This is the maximum amount of space the web cache will utiize on the storage device.

Note

The size of this cache should be at least as big as the ***Cache size*** *on the* ***Main*** *tab and not more than 90% of the total size of the storage area.*

Select the **Device** or partition on the device, click **Submit**.

Network storage share

Note

Network Storage *and* ***Local Storage*** *cannot be used at the same time. Enabling one will automatically disable the other.*

A network share is a shared folder or drive on a local Windows PC, or a PC running another operating system capable of SMB sharing (such as a Linux PC running the SAMBA service).

Refer to your operating system's documentation for details on creating a network share. What follows are some basic instructions for creating a network share under Windows XP.

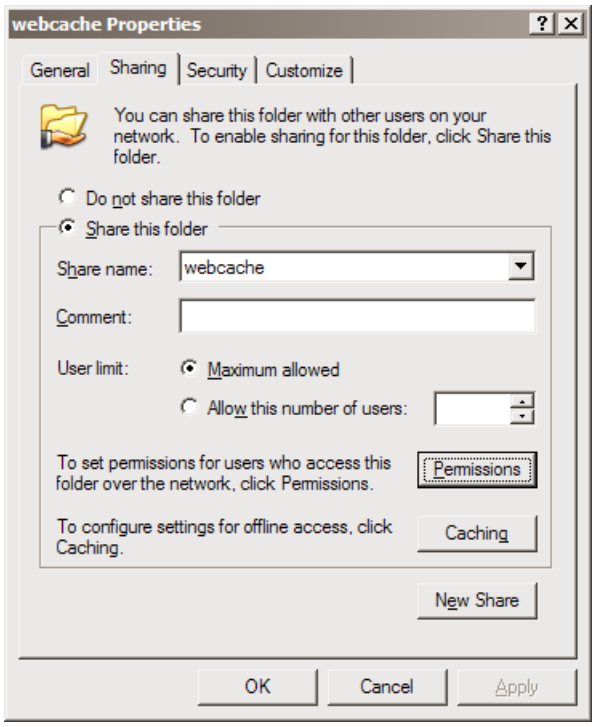
- Create a new user account:

Note

We recommend that you create a special user account to be used by the SG unit for reading and writing to the network share. If you have an existing account or wish to may the network share readable and writeable by everyone, you may skip the next step.

To create an account, click **Start** -> **Control Panel** -> **User Accounts** -> **Create a new account**. Type a name for the new account, e.g. *sguser*, and click **Next**. Typically it is sufficient to grant this account **Limited** privileges. Click **Create Account** to create it. Select the account you have just create under **Pick an account to change**. Select **Create a password**. Enter and confirm a password for this account, as well as a password hint if desired.

- Create the network share:



Launch Windows Explorer (**Start** -> **(All) Programs** -> **Accessories** -> **Windows Explorer**) and open up a folder or drive to dedicate as a network share for use by the SG unit's web cache.

Begin by disabling simple file sharing for this folder. From the **Tools** menu, select **Folder Options**. Click the **View** tab and under the **Advanced settings** section *uncheck* **Use simple file sharing (Recommended)**. Click **OK**.

Next, share the folder. Right click on the folder and select **Sharing and Security**. Select **Share this folder** and note the **Share name**, you may change this to something easier to remember if you wish.

Finally, to set the security permissions of the newly created network share, click **Permissions**.

If you wish to secure the network share with a username and password (recommended), click **Add** and type the user name the account to be used by the SG unit and click **Check Names** then **OK**.

Select this account, or **Everyone** if you are not securing the network share with a username and password, and check **Allow** next to **Full Control**. Click **OK** and **OK** again to finish.

- Set the SG unit to use the network share

Under the **Network Share** tab, check **Use share**. Enter the location of the network share in the format:

```
\\HOSTNAME\sharename
```

Enter the maximum size for the cache in **Cache size**.

Warning

*The size of this cache should be at least as big as the **Cache size** on the **Main** tab and not be more than 90% of the space available to the network share.*

Enter the **Username** and **Password** for a user that can read and write to the network share. If you allowed **Full Control** to **Everyone**, you may leave these blank.

Set up LAN PCs to use the web cache

Once the web cache has been set up, PCs on the LAN must have their browsers configured appropriately.

In Internet Explorer, select **Internet Options** from the **Tools** menu. Select the **Connections** tab and click **LAN Settings**. Under **Proxy Server**, check **Use proxy server…** and enter the IP address of your SG unit in **Address**.

Note

The SG unit's web cache uses port 3128 *by default.*

Enter *3128* in **Port**, select **Bypass proxy for local addresses** and click **OK**.

Peers

The SG unit's web cache can be configured to share cached objects with, and access objects cached by, other web caches.

Web caches communicate using the Internet Cache Protocol (ICP). ICP is used to exchange hints about the existence of URLs in neighbour caches. Caches exchange ICP queries and replies to gather information to use in selecting the most appropriate location from which to retrieve an object.

Click **Advanced**, **Peers**, then **New**.

First of all, the messages transmitted by a cache to locate a specific object are sent to **Sibling** caches, which are placed at the same level in the hierarchy. Then, the caches placed at the **Parent** level are queried if the replies from sibling caches did not succeed.

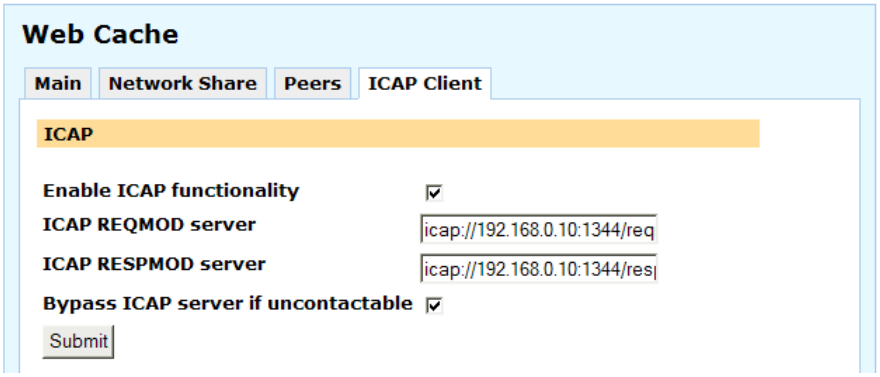
Enter the host or IP address of an ICP capable web cache peer in **Host**, then select its relationship to the SG unit's web cache (as described above) from **Type** and click **Apply**.

ICAP client

The SG unit's ICAP client allow you to utilise a third-party ICAP server as an intermediary between LAN PCs browsing the web and/or traffic incoming from the web. Outgoing web requests or incoming web traffic is passed off to the ICAP server for processing before being returned to the requesting LAN PC.

The ICAP server may process outgoing web requests from a LAN PC using a *REQMOD* service, or incoming web traffic from an external web server using a *RESPMOD* service. A typical function of a REQMOD service would be URL filtering, a typical function of a RESPMOD service would be virus scanning.

Click **Advanced** then **ICAP Client**.



Check **Enable ICAP functionality** to enable the ICAP features of the SG unit's web cache.

ICAP REQMOD server is the URL for an ICAP server's REQMOD service. This allows an ICAP server to modify web transaction requests, i.e. to process as they are being initially requested by the LAN PC, e.g. for URL filtering. It must begin with *icap://*, e.g.: *icap://192.168.0.10:1344/reqmod*

ICAP RESPMOD server is the URL for an ICAP server's RESPMOD service. This allows an ICAP server to modify web transaction responses, i.e. to process traffic that is returned from an external web server, e.g. for virus scanning. It must begin with *icap://*, e.g.: *icap://192.168.0.10:1344/respmod*

You may choose to **Bypass ICAP server if uncontactable**. If the ICAP server is not responding to requests, web transactions are allowed as normal. If this is option disabled, all web transactions are blocked until the ICAP server becomes contactable.

Advanced

Click **Advanced** then **Advanced** again to modify the advanced settings of the web cache.

You may specify the TCP network **Port** that the web cache listens on, this is usually 3128 or 8080.

Extra diagnostic output may be displayed in the system log in addition to the usual cache log file.

Objects larger than the **Maximum cached object size (KB)** are NOT be cached. If you wish to get a high BYTES hit ratio, you should probably increase this (one 32 MB object hit counts for 3200 10KB hits). If you wish to increase speed more than your want to save bandwidth you should leave this low.

Objects larger than the **Maximum cached object size in memory (KB)** are NOT kept in the memory cache. This should be set high enough to keep objects accessed frequently in memory to improve performance whilst low enough to keep larger objects from hoarding cache memory.

The **Anonymity Level** controls the amount of identifying information to be removed from web requests in order to protect your anonymity. The levels of protection are specified in increasing order and all but the first violate the HTTP standard and thus might cause problems with some web sites. The **Custom** setting is for users who have manually edited these settings in the cache configuration file as it leaves the settings untouched.

Log File Size (KB) is the maximum size of each log file before it gets rotated. If set to zero, the log files are rotated every time they're checked.

Log File Rotation Time (minutes) specifies how often the logs are checked for rotation.

Log File Rotations specifies how many log file rotations should be stored. The minimum default of 1 means 2 files will be kept: the current log file and the previous log file. The maximum of 9 will mean 10 files will be kept.

Web cache with access control

To allow the web cache to operate simultaneously with access controls, including content filtering and anti-virus, you must make some configuration changes.

Select **Advanced** from the **System** menu, click the **Configuration Files** tab. Click the **Modify** icon for **squid.conf**.

Add the following three lines anywhere in the file:

```
cache_peer 127.0.0.1 parent 81 0 no-query default
acl authd proto HTTP
never_direct allow authd
```

Click **Finish**.

Transparent web cache with access control

You may choose to have the web cache and acess controls, including content filtering and anti-virus, operate transparently. Transparent operation filters and caches web traffic regardless of whether or not the clients on the LAN have specified an HTTP proxy in their web browsers.

Select **Packet Filtering** from the **Firewall** menu, and click the **Custom Firewall Rules** tab. Add the following **Custom Firewall Rules**:

```
iptables -t nat -D ContFilt -p tcp --dport 80 -j REDIRECT --to-port 81
iptables -t nat -A ContFilt -p tcp --dport 80 -j REDIRECT --to-port 3128
```

Click **Update**.

Select **Advanced** from the **System** menu, click the **Configuration Files** tab. Click the **Modify** icon for **squid.conf**.

Add the following seven lines anywhere in the file:

```
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
cache_peer 127.0.0.1 parent 81 0 no-query default
acl authd proto HTTP
never_direct allow authd
```

Click **Finish**.

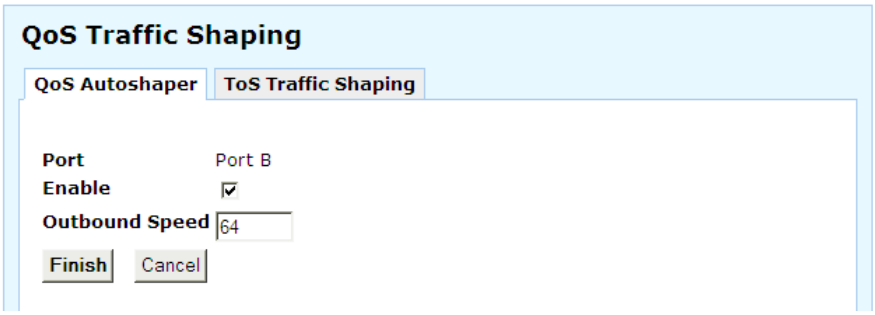
QoS Traffic Shaping

This advanced feature is provided for expert users to fine tune their network connections. Traffic shaping allows you to give preference to certain types of network traffic to maintain quality of service when a network connection is under heavy load.

QoS autoshaper

The **Auto Traffic Shaper** uses a set of inbuilt traffic shaping rules to attempt to ensure low latency on interactive connections, while maintaining fast throughput on bulk transfers.

Click **Edit** next to the network interface on which you wish to enable the autoshaper.



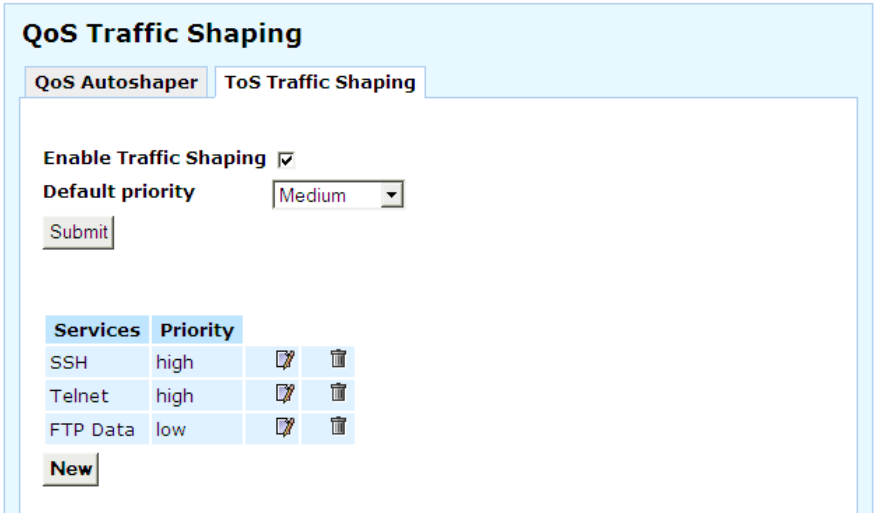
Click **Enable** and enter the **Outbound Speed** (upstream speed) of this interface's network connection in megabits per second. Click **Finish**.

Note

If you have a PPTP or PPPoE connection to the Internet, enter approximately 80 – 90% of the speed that the ISP supplied to account for protocol overheads.

ToS traffic shaping

Traffic shaping provides a level of control over the relative performance of various types of IP traffic. The traffic shaping feature of your SG unit allows you to allocate **High**, **Medium**, or **Low** priority to the following services such as **domain (tcp)**, **domain (udp)**, **ftp**, **ftp-data**, **http**, **https**, **imap**, **irc**, **nntp**, **ntp**, **pop3**, **smtp**, **ssh**, and **telnet**.



Check **Enable Traffic Shaping**, select a **Default priority** and click **Submit** to enable this feature. The **Default priority** is assigned to all network services other than those specifically added below.

To add a service, click **New** then **New** again. Select the **Protocol** and **Port** on which this service runs. Select **Priority** for this service click **Finish**.

IPv6

Check **Enable IPv6** to enable IPv6 routing and packet filtering. Support for IPv6 is currently limited.

Note

You must also enable IPv6 for each connection that supports IPv6. See the section entitled Direct Connection *towards the beginning of this chapter.*

When IPv6 is enabled, site-local addresses are assigned to LAN connections, the site-local DNS server address (**`fec0:0:0:ffff::1/64`**) is assigned to LAN connections if the DNS proxy is enabled, router advertisements are sent on LAN connections and 6to4 tunnels are created on Internet connections.

Additionally, a default set of IPv6 packet filter rules are enabled. These rules are *stateless* (as opposed to the IPv4 packet filter rules which are stateful). The default rules only support a single LAN connection and a single WAN connection. These rules may be customized, refer to the *Custom Firewall Rules* section of the chapter entitled *Firewall*.

SIP

Note

SG565, SG575, SG580, SG635 and SG710 only.

The SG's SIP proxy allows SIP software clients (like kphone, linphone, SJphone) or SIP hardware clients (Voice over IP phones which are SIP-compatible, such as those from Cisco, Grandstream or Snom) to work from a private network (such as your LAN) behind a masquerading firewall (such as the one on the SG).

SIP (Session Initiation Protocol, RFC3261) is the protocol of choice for most VoIP (Voice over IP) phones to initiate communication. By itself, SIP does not work from behind masquerading firewalls, as the transfered data contains IP addresses and port numbers.

Note

If you use an external SIP service just as the Gizmo Project or Skype, you typically do not need to use the SIP proxy. These services use STUN (Simple Traversal of UDP through NATs) to facilitate communication from behind a masquerading firewall.

The SIP proxy listens on UDP port 5060 for SIP requests (this is the standard SIP port and should not generally need to be changed), and UDP ports 7070-7079 for RTP traffic (the actual voice data).

Configuring the SIP proxy

Check **Enabled**.

The **Outbound Interface** is typically the **LAN** interface. This is the interface connected to your private network on which SIP clients are located.

The **Inbound Interface** is typically the **Internet** interface. This is the interface through which remote SIP clients can be reached.

Click **Submit**.

Details of incoming and outgoing calls are logged under **Diagnostics** -> **System Log**.

4. Firewall

The SG unit is equipped with a fully featured, stateful firewall. The firewall allows you to control both incoming and outgoing access, so that PCs on local networks can have tailored Internet access facilities while being shielded from malicious attacks from external networks.

The SG unit's stateful firewall keeps track of outgoing connections (e.g. a PC on your LAN requesting content from a server on the Internet) and only allows corresponding incoming traffic (e.g. the server on the Internet sending the requested content to the PC).

By default, your SG unit allows network traffic as shown in the following table:

Incoming Interface	Outgoing Interface	Action
LAN	Any	Accept
VPN	Any	Accept
Dialin	Any	Accept
DMZ	Internet	Accept
DMZ	Any except Internet	Drop
Internet	Any	Drop
Guest	Any	Drop

Sometimes it is useful to allow some incoming connections, e.g. if you have a mail or web server on your LAN or DMZ that you want to be accessible from the Internet. This is accomplished using a combination of NAT and packet filter rules.

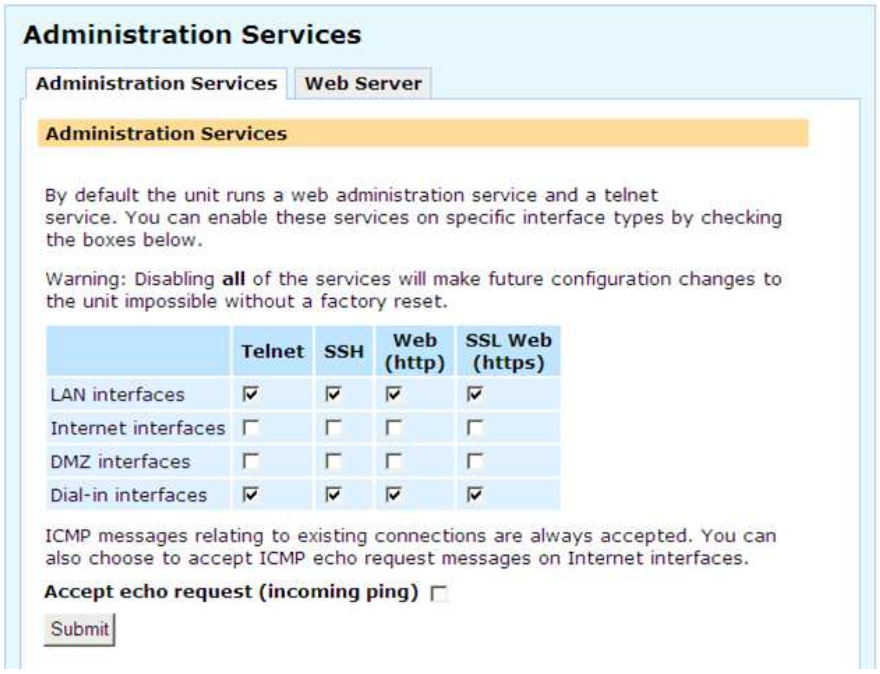
The SG unit web management console provides a powerful interface for tailoring your firewall to your network. For details, refer to the Customizing your Firewall section later in this chapter.

Incoming Access

The **Incoming Access** section allows you to control access to the SG unit itself, e.g. for remote administration. Click **Incoming Access** under **Firewall** on the main menu to display the **Incoming Access** configuration page.

Administration services

The following figure shows **the Administration Services** page:


Administration Services
Administration Services
Web Server
Administration Services
By default the unit runs a web administration service and a telnet service. You can enable these services on specific interface types by checking the boxes below.
Warning: Disabling all of the services will make future configuration changes to the unit impossible without a factory reset.
Telnet
SSH
Web (http)
SSL Web (https)
LAN interfaces
Internet interfaces
DMZ interfaces
Dial-in interfaces
ICMP messages relating to existing connections are always accepted. You can also choose to accept ICMP echo request messages on Internet interfaces.
Accept echo request (incoming ping)
Submit

By default the SG unit runs a web administration server, a Telnet and an SSH service. Access to these services can be restricted to specific interfaces.

Typically, access to the web management console (**Web**/**SSL Web**) is restricted to hosts on your local network (**LAN Interfaces**).

Disallowing all services is not recommended, as this makes future configuration changes impossible unless your SG unit is reset to the factory default settings.

Warning

*If you do want to allow administrative access on interfaces other than **LAN Interfaces**, there are several security precautions you should take. See the note in the next section for details. Also consider remote administration using a VPN connection as an alternative to opening a hole in the firewall, PPTP in particular is well suited to this task.*

You can also select to **Accept echo request (incoming port)** on Internet interfaces. The default is to disallow echo requests, so your SG unit does not respond to pings on its Internet interfaces. This may make it more difficult for external attackers scanning for hosts to discover your SG unit. Destination unreachable ICMP messages are always accepted.

Web Server

Click the **Web Server** tab to configure the SG unit's administrative web server. This web server is responsible for running the web management console.

Here you can change the port on which the server runs. Most SG units support enabling SSL encryption for establishing secure connections to the web management console from SSL enabled browsers.

Web Server
Administration Services
Web Server
Web Server
Upload SSL Certificates
Create SSL Certificates
Web Server
The unit can be configured to run its web admin server on a port other than the HTTP default (80). Changing the default administration port is recommended if you intend to allow the unit to be configured externally, not just from the trusted (LAN) side on your network.
Note: To continue web configuration you will need to point your browser to the unit's new administration port (e.g. a device at IP address 10.0.0.1 using administration port 81 is http://10.0.0.1:81/)
Web server port 8088
Submit

Note

Changing the web server port number is recommended if you are allowing Internet access to the Management Console. This may help hide the web management console from casual web surfers who type your SG unit's Internet IP address into a web browser.

Ideally, you should use packet filter rules (see the Packet Filtering *section later in this chapter) to restrict who has access for remote administration (i.e. allow connections on the administrative web server port from trusted originating IP addresses only).*

By default, the web management console runs on the default HTTP port (i.e. 80).

After changing the web server port number, you must include the new port number in the URL to access the pages. For example, if you change the web administration to port number 88, the URL to access the web administration is similar to**:** http://192.168.0.1:88

SSL/HTTPS (Secure HTTP)

Note

Not available on the SG300, SG530, SG570 or SG630.

To enable SSL support on the SG unit, an RSA x509 certificate as well as its private key are required. These may be uploaded to the SG unit, or you may choose to have the SG unit create a self-signed certificate.

SSL/HTTPS Web Server Support
A valid SSL certificate has not been installed
To access the web pages via SSL encryption, the URL becomes https:// instead of http:// (e.g. https://10.0.0.1)
The web server can be configured in one of 3 ways:
Normal (http) and SSL (https) web server access
Disable SSL (https) web server access
Disable normal (http) web server access
Submit

Once valid SSL certificates have been uploaded or created, **A valid SSL certificate has been installed** is displayed. The SG administrative web server can then operate in one of one of 3 modes:

- Both **Normal (HTTP) and SSL (HTTPS) web server access**
- **Disable SSL (HTTPS) web server access** (HTTP only)
- **Disable normal (HTTP) web server access** (HTTPS only)

To access the web management console securely using SSL encryption, the URL becomes **https://** instead of **http://** (e.g. https://10.0.0.1).

Upload SSL certificates

If you have purchased or created SSL certificates for a web server, you can upload them to the SG unit under **Upload SSL certificates** tab.

Click **Browse** to locate the **Local Certificate** (RSA x509 certificate) and its corresponding **Private Key Certificate**

Create SSL certificates

To create a self-signed certificate on the SG unit, click the **Create SSL certificates** tab.

Warning

When accessing the web management console using HTTPS, your web browser may give warnings/errors about the authenticity/validity of the certificate. This is because it has not been signed by a known Certificate Authority, it is self-signed.

Select the appropriate **Country** and certificate key length from the **Generate an RSA key of** pull down menu. All other fields but **Host name (Common Name)** are optional; they are used to create the certificate's distinguished name.

Generating a certificate usually takes a few minutes, exact time depends on the model of SG unit, and the key length. When the certificate has been created, **A valid SSL certificate has been installed** is displayed under the **Web Server** tab.

Customizing the Firewall

The majority of firewall customization is typically accomplished by creating **Packet Filter** and network address translation (**NAT**) rules.

Packet filter rules match network packets based on a combination of incoming and outgoing interface, source and destination address and destination port and protocol. Once a packet is matched, it can be allowed or disallowed.

NAT rules match packets in a similar manner. However, instead of simply allowing or disallowing traffic, you may alter the source or destination address and/or port of the packet as it passes through the firewall.

A typical use of NAT rules is to forward packets destined for your Internet IP address to an internal web server or email server on your LAN. This is known as a port forward, or destination NAT as it alters the destination address of the packet.

The first step in creating packet filter or NAT rules, is to define services (such as web or email) and addresses (such as your internal web server, or a trusted external host) under **Definitions**.

Definitions

Before creating packet filter or NAT rules, it is sometimes useful to define services or groups of services, addresses and interfaces to be used to match packets.

Definitions need not be created for simple rules that only specify a single service, address or interface, as these can be entered while creating the rule.

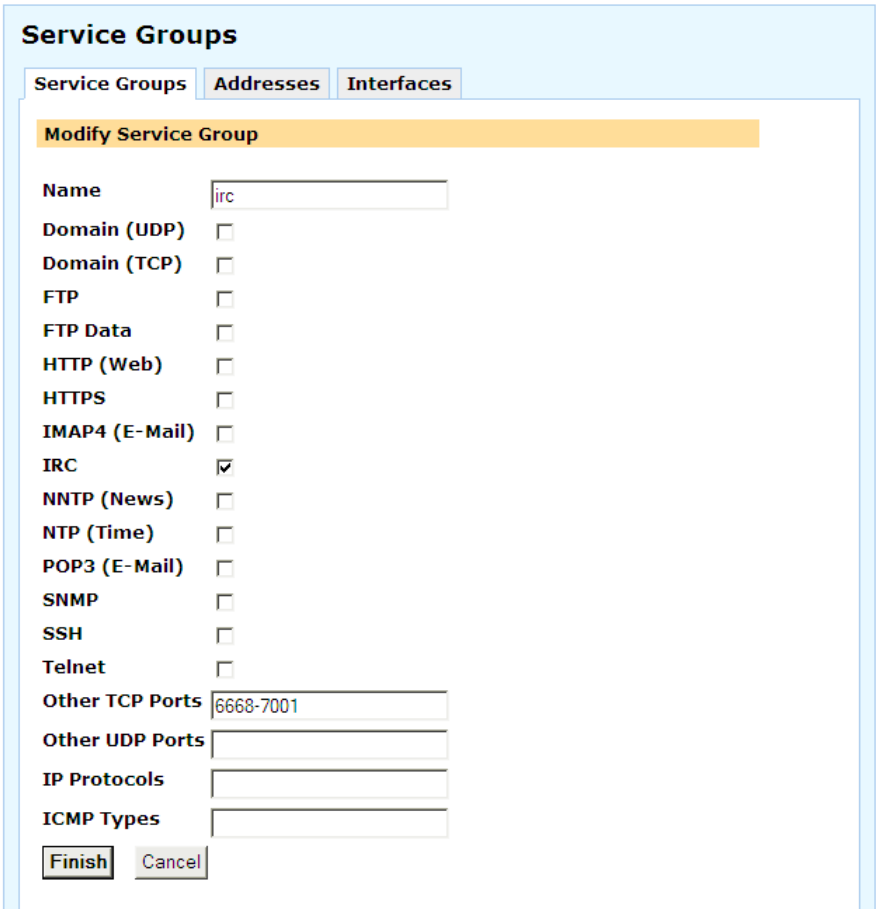
If a rule specifies groups of services, addresses or interfaces, then you must create definitions for these groups before creating the rule.

Service groups

A network service is defined by a protocol and port. Protocol may be either TCP, UDP, ICMP or IP, and port may be any valid network port number (i.e. 1 and 65535), e.g. HTTP (web) uses the TCP protocol, with a default port of 80. Network packets may be matched by destination service.

Click the **Service Groups** tab. Any services that have already been defined are displayed. Click **New** to add a new service group, or select an existing service group and click **Modify**.

Adding or modifying a service group is shown in the following figure:



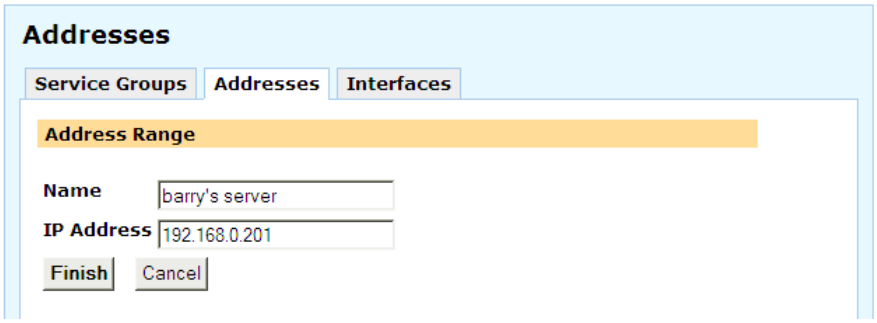
A service group can be used to group together similar services. For example, you can create a group of services that you wish to allow, and then use a single rule to allow them all at once. Select the services from the list of predefined services, or enter the port number to define a custom TCP, UDP, ICMP or IP service. A service may belong to multiple service groups.

Addresses

Addresses are a single IP address, or range of IP addresses, or a DNS hostname. Network packets may be matched by source or destination address.

Click the **Addresses** tab. Any addresses that have already been defined are displayed. Click **New** to add a new address, or select an existing address and click **Modify**. There is no need to add addresses for the SG unit's interfaces, these are predefined.

Adding or modifying an address is shown in the following figure:



You may either add a **Single Address or Range** or **DNS Hostname**. You may also group previously added addresses together by defining an **Address Group** to simplify your firewall ruleset.

Select how you would like to add the address or addresses, and click **New**. Either enter the DNS **Hostname**, the **IP Address** or address range and an optional descriptive **Name**, or select the addresses to group and enter a descriptive **Name**. Click **Finish**.

Warning

DNS hostnames are not generally recommended for enforcing security policies. They are unreliable, and may cause significant delays in updating the firewall rules.

Interfaces

Packets may also be matched by incoming and outgoing **Interface**.

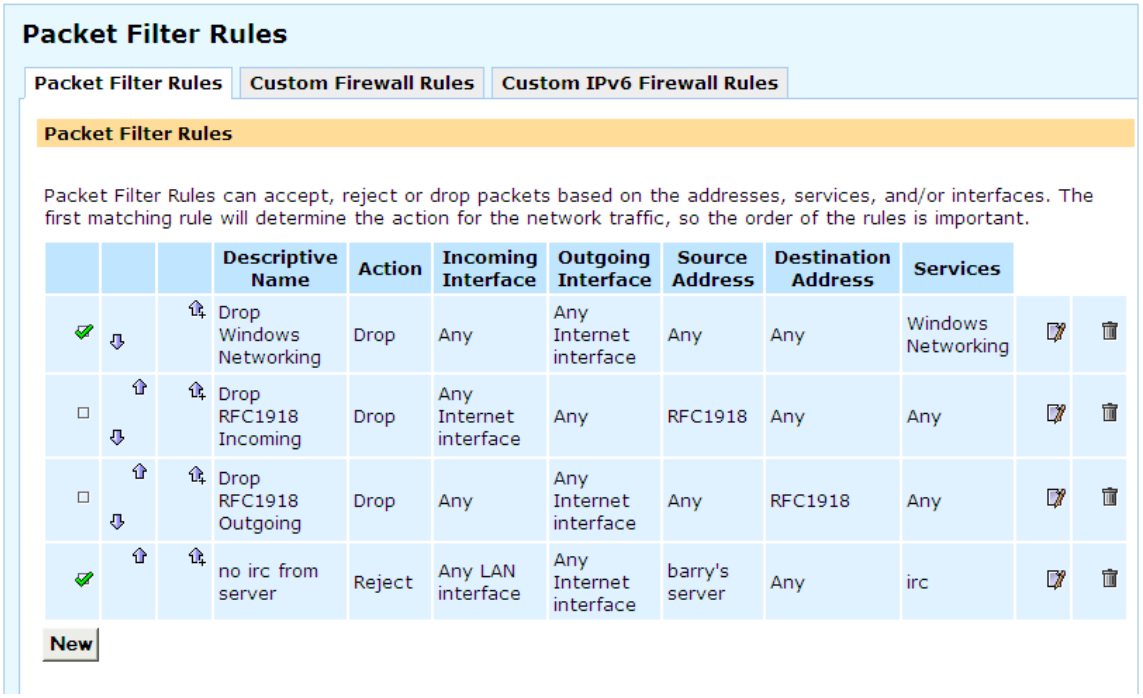
You may group the SG unit network interfaces into **Interface Group**s, to simplify your firewall ruleset. Select the interfaces to group and enter a descriptive **Name** (required). Click **Finish**.

Packet Filtering

Packet filter rules match traffic based on a combination of the source and destination address, incoming and outgoing interface, and destination service. Matched packets may be allowed or disallowed.

Packet filter rules

Click **Packet Filter Rules**.



Click **New** to add a new filter rule.

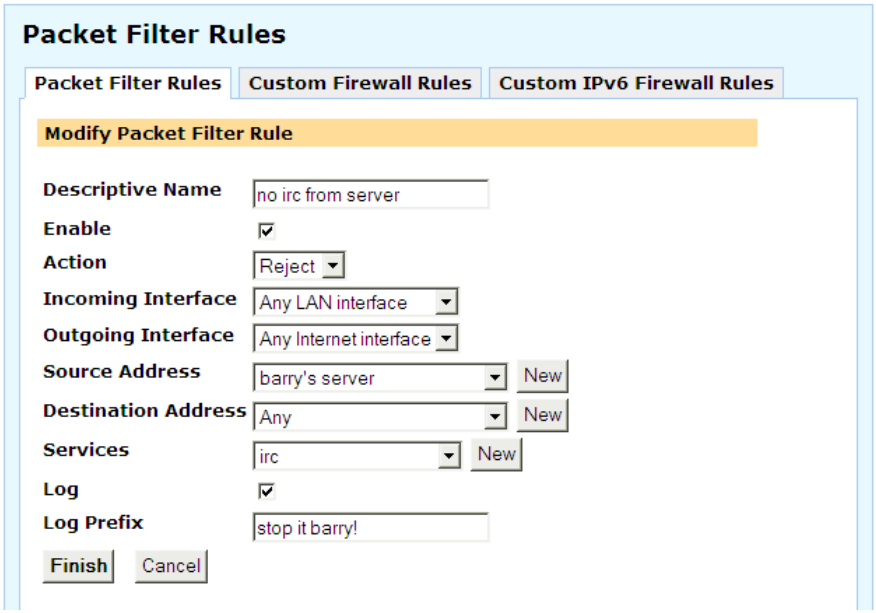
Any rules that have already been defined are displayed, you may **Edit** or **Disable/Enable** these rules by clicking the appropriate icon.

You may also add a new rule above an existing one by clicking the **Add Above** icon.

Note

*The first matching rule determines the action for the network traffic, so the order of the rules is important. You can use the **Move Up** and **Move Down** icons to change the order. The rules are evaluated top to bottom as displayed on screen.*

Adding or modifying a rule is shown in the following figure:



The **Action** specifies what to do if the rule matches.

- **Accept** means to allow the traffic.
- **Drop** means to disallow the traffic.
- **Reject** means to disallow the traffic, but also send an ICMP port unreachable message to the source IP address.
- **None** means to perform no action for this rule. This is useful for a rule that logs packets, but performs no other action.

Type controls which incoming and outgoing interface options are available.

- **Forward** means filter forwarded packets only, i.e. packets traversing the SG unit. You can select both incoming and outgoing interfaces.

- **Input** means filter packets destined for this unit. You can only select the incoming interface.

- **Output** means filter packets generated by this unit. You can only select the outgoing interface.

The **Incoming Interface** is the interface/network port that the SG unit received the network traffic on. Set this to **None** to match traffic destined for the SG unit itself.

The **Outgoing Interface** is the interface/network port that the SG unit routes the network traffic out. Set this to **None** to match traffic originating from the SG unit itself.

The **Source Address** is the address that the traffic is arriving from.

The **Destination Address** is the address that the traffic destined to.

Warning

*The previous four fields may be set to **Any**. **Any** does not match traffic sent or received by the SG unit itself, only traffic passing through it.*

The four fields above may also be set to **None** or **Any**. **None** matches requests originating from the Cyber

None matches network traffic that is destined for the SG unit itself. This is useful for controlling access to services provided by the SG unit, such as the web management console.

Note

*When adding a rule, you may either use **Predefined** addresses or services that have been added under **Definitions**, or click **New** to manually enter an address or service.*

The **Log** option controls whether to log the first packet of the connection to the SG unit's system log. You may enter a **Log Prefix** to make it easier to identify which rules are being matched when inspecting the system log.

Rate limiting

Note

Rate Limit *settings are only available when modifying rules. They cannot be specified when creating a new rule.*

Once you have created a packet filtering rule, you may specify rate limiting settings. These settings are useful for preventing a service from becoming unavailable should many connection attempts occur in a short period of time (e.g. in the case of a denial of service (DOS) attack). Packets that exceed the specified limit can be accepted, rejected or dropped, and can be logged.

Click the **Modify** icon next to the rule that you wish to rate limit, and click the **Rate Limit** tab.

Check **Enable Rate Limiting** for this rule.

Rate (per second) is the average number of connections that will be matched before rate limiting applies, specified as connections per second.

Note

If Access Control is enabled, then packets that traverse Access Control are rate limited separately from other packets, so that potentially twice the specified rate will be matched.

Burst is the maximum instantaneous burst of connections before rate limiting applies, specified as the number of connections. This is useful for services that require a multiple connections within a short time.

Action if Limited is the action to take when a packet matches the packet filter rule, but exceeds the rate limit.

- **None**: Perform no action for rate limited packets, and continue matching on subsequent rules. This is useful if you want rate limited packets to fall through to a more general rule.

- **Accept**: Allow the rate limited packet.

- **Reject**: Disallow the rate limited packet, but also send an ICMP protocol unreachable message to the source IP address.

- **Drop**: Silently disallow the rate limited packet.

If **Log if Limited** is checked, then first packet of any rate limited connection will generate a log message.

Log Prefix specifies the text to be placed at the start of the log message. This can be used to make it easier to identify which rules are being matched when inspecting the system log.

Custom firewall rules

The **Custom Firewall Rules** and **Custom IPv6 Firewall Rules** tabs allow firewall experts to view the current firewall rules and add custom *iptables* firewall rules.

Note

Only experts on firewalls and iptables are able to add effective custom firewall rules (further reading can be found at http://www.netfilter.org/documentation/*).*

Configuring the SG unit's firewall via the ***Incoming Access*** *and* ***Outgoing Access*** *and* ***Packet Filtering*** *configuration pages is adequate for most applications.*

Refer to *Appendix C – System Log* for details on creating custom log rules using iptables.

Network Address Translation (NAT)

Network address translation (NAT) modifies the IP address and/or port of traffic traversing the SG unit. The SG unit supports several types of network address translation.

The most common of these is **Port Forwarding** (also known as port address translation, PAT or destination NAT, DNAT). This is typically used to alter the destination address (and possibly port) of matched packets arriving on the SG unit Internet interface to the address of a host on the LAN. This is the most common way for internal, masqueraded servers to offer services to the outside world.

Source NAT rules are useful for masquerading one or more IP addresses behind a single other IP address. This is the type of NAT used by the SG unit to masquerade your private network behind its public IP address.

To a server on the Internet, requests originating from the hosts behind masqueraded interface appear to originate from the SG unit, as matched packets have their source address altered. You may enable or disable source NAT between interfaces under **Masquerading**, and fine tune source NAT rules under **Source NAT**.

1-to-1 NAT is a combination of destination NAT and source NAT. Both destination NAT and source NAT rules are created for full IP address translation in both directions. This can be useful if you have a range of IP addresses that have been added as interface aliases on the SG unit's WAN interface, and want to associate one of these external alias IP addresses with a single internal, masqueraded computer. This effectively allocates the internal computer its own real world IP address, also known as a *virtual DMZ*.

Port forwarding

Port forwarding rules alter the destination address and optionally the destination port of packets received by the SG unit.

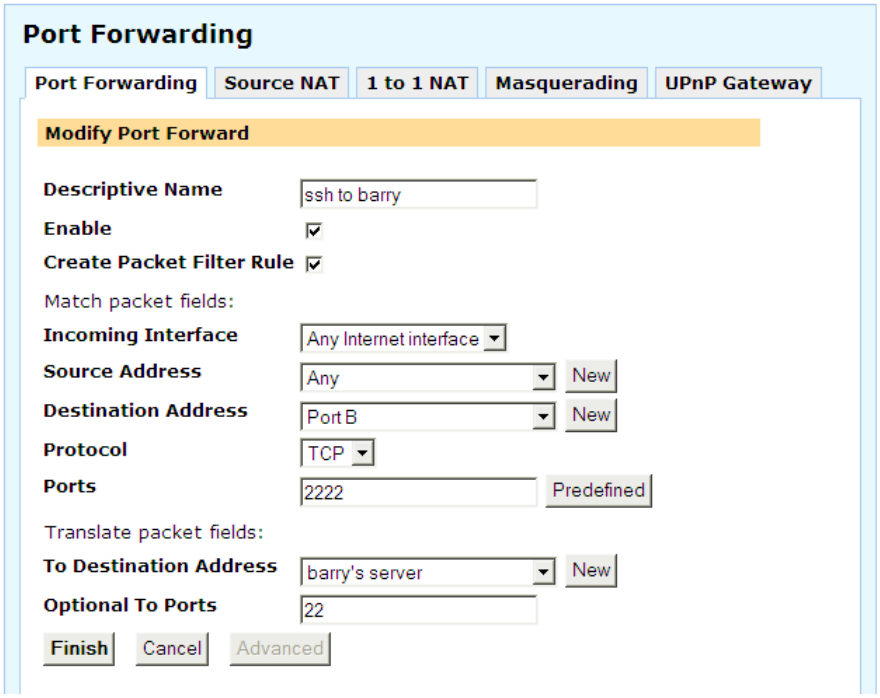
Port forwarding allows controlled access to services provided by machines on your private network to users on the Internet by forwarding requests for a specific service coming into one of the SG unit's interfaces (typically the WAN interface) to a machine on your LAN, which services the request.

Click **Port Forwarding**. Any rules that have already been defined are displayed, you may **Edit** or **Disable/Enable** these rules by clicking the appropriate icon. Click **New** to add a new rule.

You may also add a new rule above an existing one by clicking the **Add Above** icon, or below with **Add Below**.

Note

*The first matching rule determines the action for the network traffic, so the order of the rules is important. You can use the **Move Up** and **Move Down** icons to change the order. The rules are evaluated top to bottom as displayed on screen.*



Note

*The example shown in the screenshot above forwards the SSH (secure shell) protocol to an internal server (*barry's server*). SSH allows encrypted remote access, typically to a server running Linux, BSD or another Unix-like operating system.*

In this example, port 2222 is used rather than the standard SSH port of 22, this is to allow remote access using SSH to the SG unit itself, which runs an SSH server on port 22. So a remote user connects to port 2222 on SG unit's Internet address in order to access port 22 of barry's server*.*

The following fields are displayed:

Descriptive Name	An arbitrary name for this rule
Enable	Uncheck to temporarily disable this rule
Create Packet Filter Rule	Create a corresponding packet filter rule to accept NATed packets, generally leave this checked unless you want to manually create a more restrictive filter rule through **Rules**

This rule is applied to packets that match the critera described by the next four fields.

Destination Address	The destination address of the request, this is the address that is altered
Protocol	The protocol of the packet
Ports	The destination service port or ports of the request, note that many public ports may be forwarded to a single internal port

The next two fields describe how matching packets should be altered.

To Destination Address	The address to replace the **Destination Address** (this is typically the private address of a host on the LAN)
Optional To Ports	The port to replace **Ports**, if you leave this blank the port remains unchanged, otherwise enter the port on the host at **To Destination Address** to service the request

Click **Advanced** if you want to specify the incoming interface and source address, otherwise this rule is applied to all WAN interfaces and all source addresses are matched.

Incoming Interface	The interface that receives the request
Source Address	The address from which the request originated (for port forwarding you may specify this to restrict the internal service to be only accessible from a specific remote location)

Note

*When adding a rule, you may either use **Predefined** addresses or services that have been added under **Definitions**, or click **New** to manually enter an address or service.*

Port forwarding to an internal mail server

The following is an example of using port forwarding to allow hosts on the Internet to send and receive mail using a mail server on your LAN.

Warning

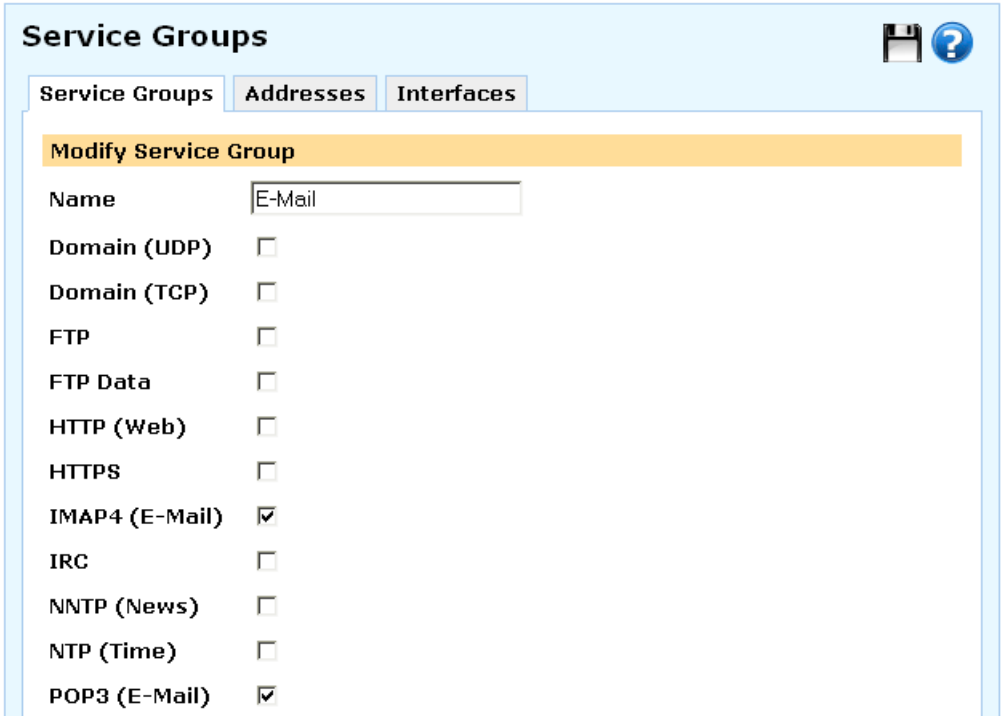
Precautions must be taken when configuring the mail server, otherwise you become susceptible to such abuse as unauthorized relaying of unsolicited email (spam) using your server. Configuration of the email server is outside the scope of this manual.

Where possible, add packet filter rules to restrict access to the internal email server to trusted external hosts only.

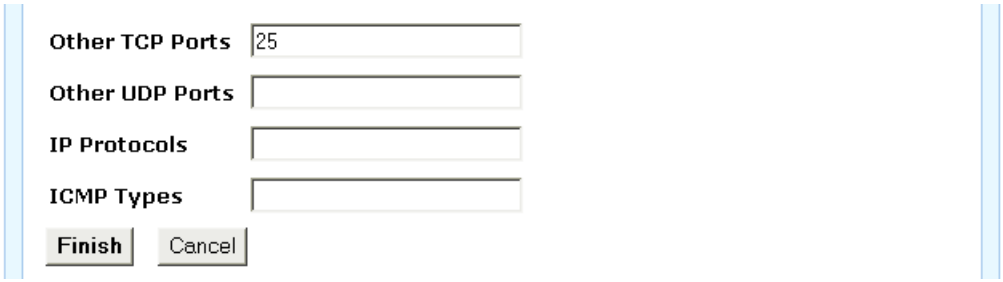
First, add a service group to group email services (SMTP, POP3 and IMAP).

Click **Definitions**, the **Service Groups** tab, then **New**.

Enter *E-Mail* in **Name**.



Check one or both of **IMAP4 (E-Mail)** if your server supports IMAP mail retrieval and **POP3 (E-Mail)** if your server supports POP3 mail retrieval.

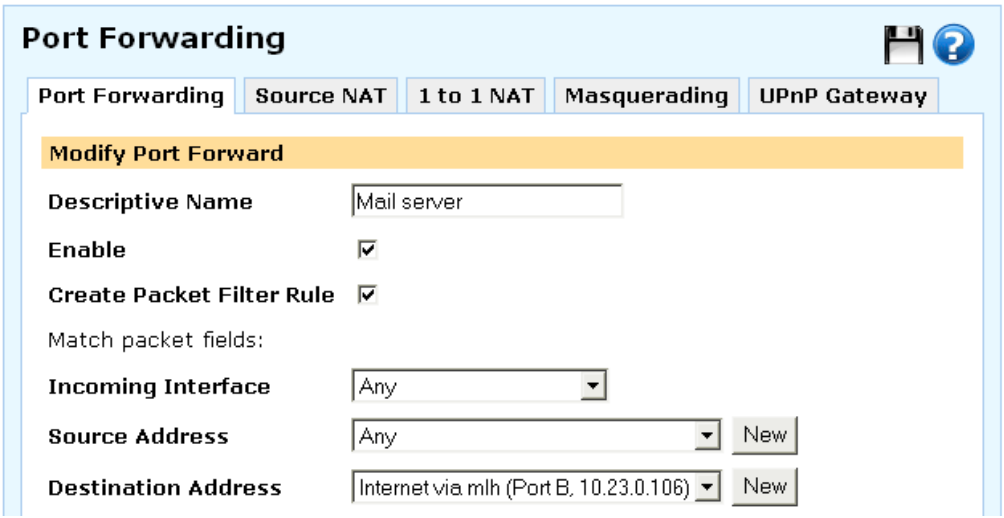


Enter *smtp* in **Other TCP Ports**. This is the protocol remote clients use for sending mail via the server.

Click **Finish**.

Click **NAT**, the **Port Forwarding** tab, then **New**.

Click **Advanced** at the bottom of the page.



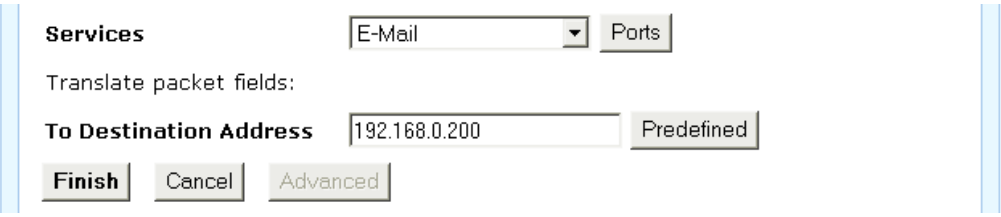
Enter *Mail server* In **Descriptive Name**.

Leave **Enable** and **Create Packet Filter Rule** checked.

Leave **Incoming Interface** and **Source Address** as **Any**.

Select your Internet connection in **Destination Address**.

Click **Predefined** next to **Services**.



Select **E-Mail** from **Services**.

Enter your internal email server's IP address in **To Destination Address**.

Click **Finish**.

Configure mail clients on the Internet with the SG unit's Internet IP address as the server to use for sending (SMTP) and receiving (POP3 or IMAP) mail. If your SG unit has a dynamic Internet IP address, consider using a dynamic DNS server; see *Dynamic DNS* in the *DNS* section of the chapter entitled *Network Setup*.

Source NAT

Source NAT alters the source address of packets received by the SG unit. This is typically used for fine tuning the SG unit's masquerading behaviour.

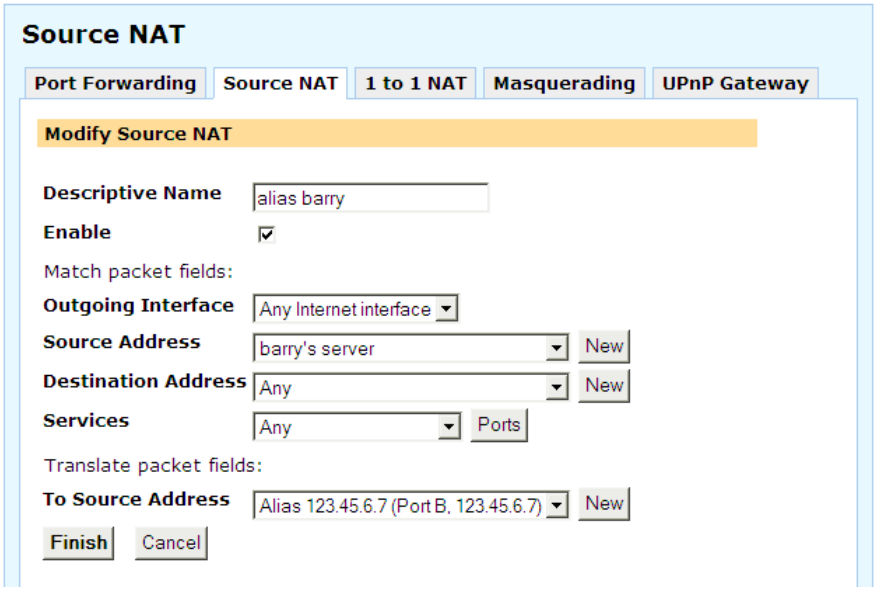
See the *Masquerading* section later in this chapter for information on altering the basic masquerading relationships between your SG unit's interfaces.

Click **Source NAT**. Any rules that have already been defined are displayed, you may **Edit** or **Disable/Enable** these rules by clicking the appropriate icon. Click **New** to add a new rule.

You may also add a new rule above an existing one by clicking the **Add Above** icon, or below with **Add Below**.

Note

*The first matching rule determines the action for the network traffic, so the order of the rules is important. You can use the **Move Up** and **Move Down** icons to change the order. The rules are evaluated top to bottom as displayed on screen.*



The following fields are displayed:

Enable	Uncheck to temporarily disable this rule
Descriptive Name	An arbitrary name for this rule

This rule is applied to packets that match the critera described by the next four fields.

Outgoing Interface	The interface that the packet to masquerade behind, typically **Internet**
Source Address	The address from which the request originated, typically be a private address on the LAN or DMZ
Destination Address	The destination address of the request
Services	The destination service port or ports of the request

The next field describes how matching packets should be altered.

To Source Address	The address to replace the **Source Address**, this is typically a public address of the SG unit, i.e. **Internet** or **Outgoing Interface Address**

Note

*When adding a rule, you may either use **Predefined** addresses or services that have been added under **Definitions**, or click **New** to manually enter an address or service.*

1-to-1 NAT

This creates both a source NAT and destination NAT rule for mapping all services on an internal, private address to an external, public address.

Note

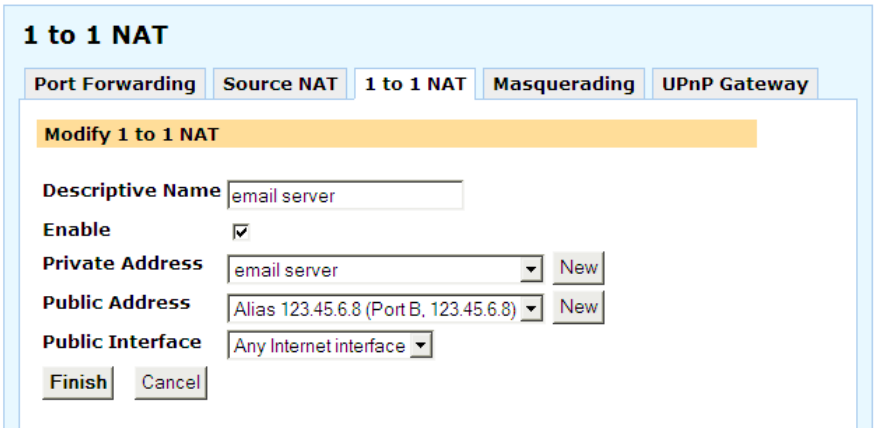
After adding a 1-to-1 NAT rule, you must manually create packet filter rules to allow incoming packets on the public address.

Click **Source NAT**. Any rules that have already been defined are displayed, you may **Edit** or **Disable/Enable** these rules by clicking the appropriate icon. Click **New** to add a new rule.

You may also add a new rule above an existing one by clicking the **Add Above** icon, or below with **Add Below**.

Note

*The first matching rule determines the action for the network traffic, so the order of the rules is important. You can use the **Move Up** and **Move Down** icons to change the order. The rules are evaluated top to bottom as displayed on screen.*



The following fields are displayed:

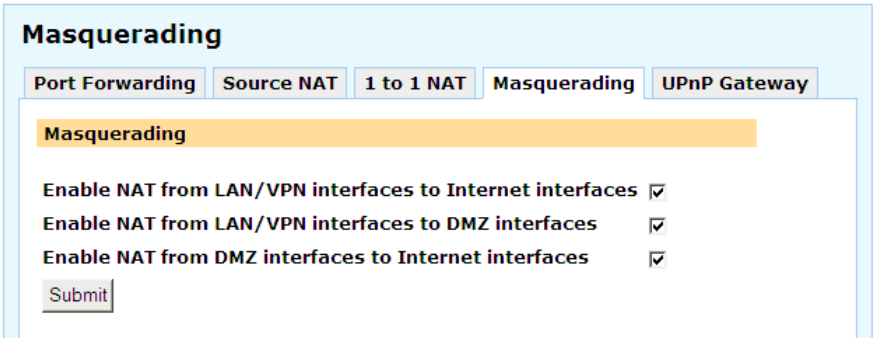
Descriptive Name	An arbitrary name for this rule
Enable	Uncheck to temporarily disable this rule
Private Address	The private address to change
Public Address	The public address, typically a WAN interface alias
Public Interface	Select the interface on which the public address resides, this is typically **Internet**

Note

*When adding a rule, you may either use **Predefined** addresses that have been added under **Definitions**, or click **New** to manually enter an address.*

Masquerading

Masquerading is a form of source network address translation (NAT). It translates many addresses (such as private LAN IP addresses) into a single address (such as the external Internet IP address).



Masquerading has the following advantages:

- All machines on the local network can access the Internet using a single ISP account.
- Only one public IP address is used and is shared by all machines on the local network. Each machine has its own private IP address.

The firewall remains active when masquerading is disabled.

Note

The displayed options apply to the firewall classes, not to the ports with these names. That is, the LAN interface options apply to all interfaces that are configured with a LAN connection type, not just to the port labelled as LAN.

*It strongly recommended that you leave **Enable NAT from LAN/VPN interfaces to Internet interfaces** checked. Typically, this is required to allow Internet access from the LAN.*

Universal plug and play gateway

The Universal Plug and Play (UPnP) Gateway allows UPnP capable applications and devices to request port forwarding rules to be established on demand. This allows some applications and devices that may not operate correctly behind the NAT firewall to automatically work.

Warning

When UPnP in enabled, any host connected to the internal network can create a port forwarding rule on the firewall. We strongly recommend that do not enable the UPnP Gateway feature.

Configuring the UPnP gateway

The UPnP Gateway needs to be run on a pair of interfaces, the **External interface** (typically **default gateway internet**) and the **Internal interface** (typically **LAN** or **DMZ**).

The UPnP Gateway sends out notifications on the internal interface, advertising its presence on the network. Any UPnP capable applications or devices that you require to make use of the UPnP Gateway need to be connected to the SG unit via this interface. The UPnP Gateway listens on this interface to requests from UPnP capable applications and devices to establish port forwarding rules.

In response to these requests, the UPnP Gateway establishes port forwarding rules to allow matching packets to be forwarded from the configured external interface through to the internal interface.

Note

The port forwarding rules set up via the UPnP Gateway are temporary. The list of configured UPnP port forwarding rules is cleared should the SG unit be power cycled, or should the internal or external interface become unavailable.

The UPnP Gateway is intended for transitory application port forwarding, such as those established by some versions of Microsoft Messenger for file transfers. For long term port forwarding, we recommend configuring the necessary rules via the **Destination NAT** features in **Packet Filtering**.

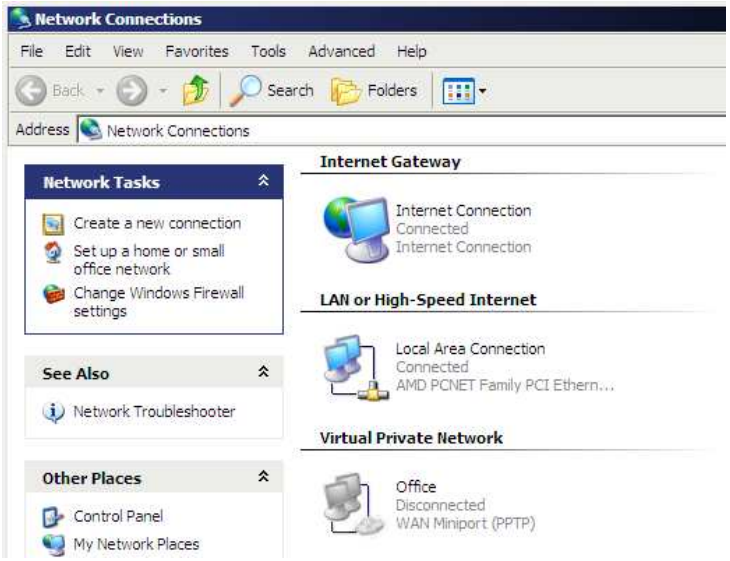
Should there be a conflict, packet filtering and NAT rules have priority over UPnP rules.

Configuring UPnP rules from Windows XP

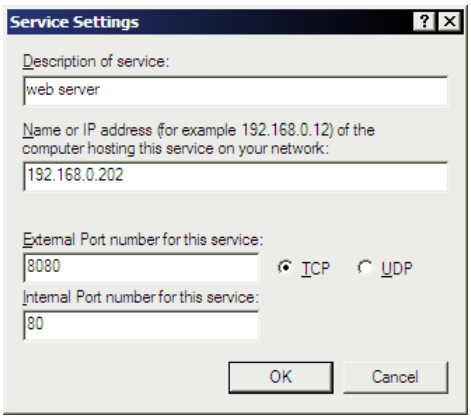
Once UPnP is running on the SG unit, you may configure UPnP port forwarding rules from a local Windows XP PC.

Ensure the Windows PC's **Default gateway** is set to the SG unit's UPnP **Internal interface**.

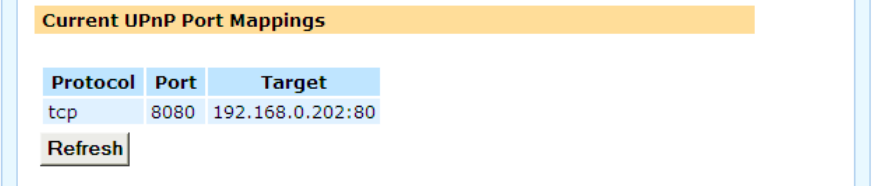
After 10 to 15 seconds, a new connection named **Internet Connection** appears in the Windows PC's **Network Connections** folder.



Open **Internet Connection**, click **Settings** then **Add**.



Enter an arbitrary **Description of service**, the **Name or IP address of the computer hosting this service on your network**, the **External Port number for this service** and the **Internal Port number for this service**. Select whether the service uses the **TCP** or **UDP** protocol. Click **OK**.



This rule now appears on the SG unit UPnP page, under **Current UPnP Port Mappings**.

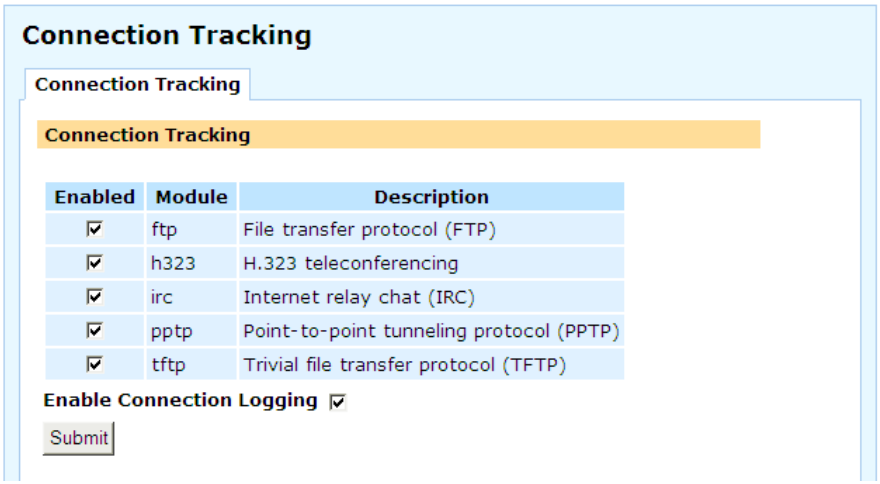
Connection Tracking

Connection tracking keeps a record of what packets have passed through the unit, and how they relate to each other. A sequence of related packets is called a connection. This is required for stateful packet filtering and network address translation (NAT).

Most packets are correctly handled by generic support for protocols such as TCP and UDP. However, some protocols are more complicated and require specific connection tracking modules in order to record the state correctly. For example, FTP requires additional connections for data transfer, and also transmits IP addresses and ports within the data portion of packets.

Configuring connection tracking

You can select which connection tracking modules are used by checking the **Enabled** option. Since connection tracking modules can allow additional connections through the firewall, you should disable modules that you do not need.



Note

Implementations of protocols such as H.323 can vary, so if you are experiencing problems then you can try disabling the module.

Check **Enable Connection Logging** to log connections to the system log as they are established and expire, however this may result in a lot of log messages if you have a large or busy network.

Intrusion Detection

Note

The SG300, SG530, SG550, SG560, SG570 and SG630 provide Basic Instrusion Detection and Blocking *only.*

The SG unit provides two intrusion detection systems (IDS): the lightweight and simple-to-configure *Basic Intrusion Detection and Blocking*, and the industrial strength *Advanced Intrusion Detection and Prevention*.

These two systems take quite different approaches. Basic Intrusion Detection offers a number of dummy services to the outside world, which are monitored for connection attempts. Clients attempting to connect to these dummy services can be blocked. *Advanced* Intrusion Detection uses complex rulesets to detect known methods used by intruders to circumvent network security measures, which it either blocks, or logs to a remote database for analysis.

Read on to find out how using an IDS can benefit your network's security, or skip ahead to the *Basic* or *Advanced Intrusion Detection* section for an explanation of configuration options.

The benefits of using an IDS

External attackers attempting to access desktops and servers on the private network from the Internet are the largest source of intrusions. Attackers exploiting known flaws in operating systems, networking software and applications, compromise many systems through the Internet.

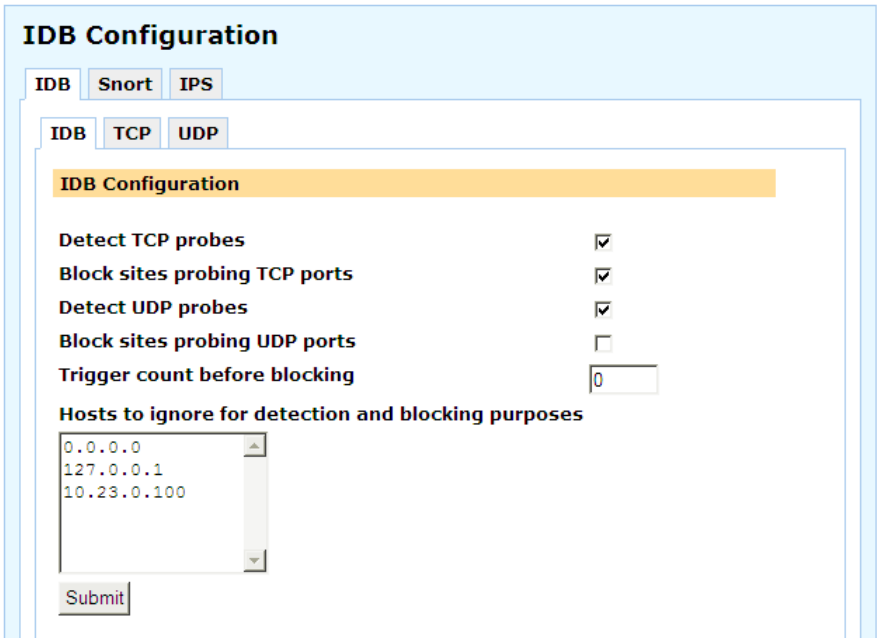
Generally firewalls are not granular enough to identify specific packet contents that signal an attack based on a known system exploit. They act as a barrier analogous to a security guard screening anyone attempting to enter and dismissing those deemed unsuitable, based on criteria such as identification. However identification may be forged. On the other hand intrusion detection systems are more like security systems with motion sensors and video cameras. Video screens can be monitored to identify suspect behaviour and help to deal with intruders.

Firewalls are often easily by-passed through well-known attacks. The most problematic types of attacks are tunnelling-based and application-based. The former occurs when an attacker masks traffic that should be normally screened by the firewall rules by encapsulating it within packets corresponding to another network protocol. Application-based attacks occur when vulnerabilities in applications can be exploited by sending suspect packets directly with those applications.

These attacks can potentially be detected and prevented using an intrusion detection system.

Basic Intrusion Detection and Blocking (IDB)

Click the **IDB** tab to configure basic Intrusion Detection and Blocking (IDB).



IDB operates by offering a number of services to the outside world that are monitored for connection attempts. Remote machines attempting to connect to these services generate a system log entry providing details of the access attempt, and the access attempt is denied.

Because network scans often occur before an attempt to compromise a host, you can also deny all access from hosts that have attempted to scan monitored ports. To enable this facility, select one or both of the block options and these hosts are automatically blocked once detected.

IDB Configuration

Detect TCP probes monitors dummy TCP services, **Detect UDP probes** monitors dummy UDP services. **Block sites probing TCP ports** and **Block sites probing UDP ports** blocks hosts attempting to connect to these services from all access to the SG unit. Connection attempts are logged under **Scanning Hosts**.

Warning

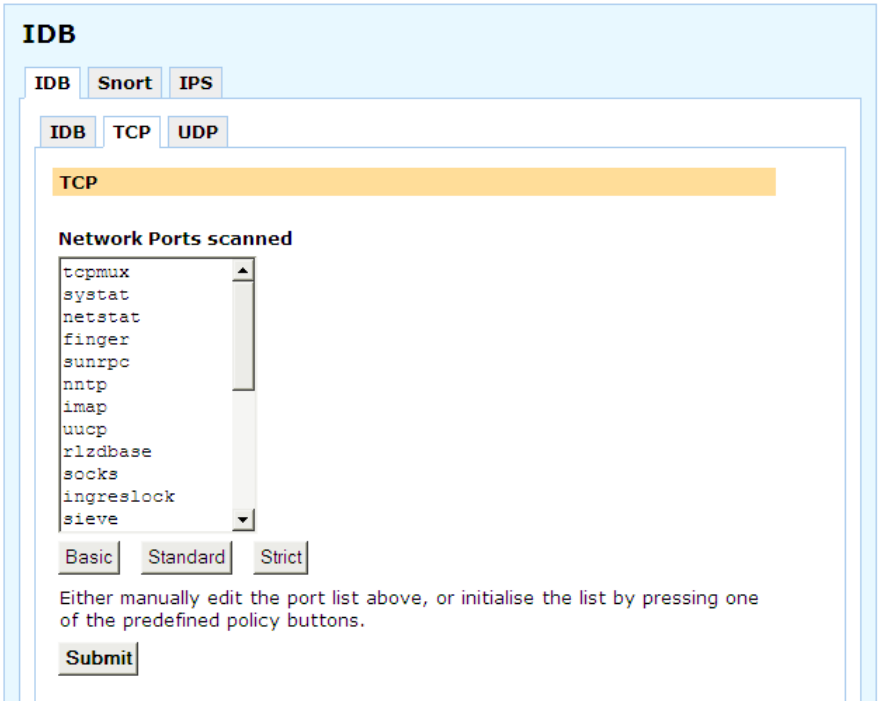
A word of caution regarding automatically blocking UDP requests. Because an attacker can easily forge the source address of these requests, a host that automatically blocks UDP probes can be tricked into restricting access from legitimate services. Proper firewall rules and ignored hosts lists significantly reduces this risk.

Trigger count before blocking specifies the number of times a host is permitted to attempt to connect to a monitored service before being blocked. This option only takes effect when one of the previous blocking options is enabled. The trigger count value should be between 0 and 2 (o represents an immediate blocking of probing hosts). Larger settings mean more attempts are permitted before blocking and although allowing the attacker more latitude, these settings reduce the number of false positives.

Hosts to ignore for detection and block purposes is a list of host IP addresses which the IDB ignores. This list may be freely edited so trusted servers and hosts are not blocked. The two addresses *0.0.0.0* and *127.0.0.1* cannot be removed from the ignore list because they represent the IDB host. You may enter the IP addresses as a range, see the IP address ranges section further on for more information.

Dummy services

Specify the dummy services to monitor under the **TDP** and **UDP** tabs. Shortcut buttons also provide pre-defined lists of services to monitor.



The **Basic** button installs a bare bones selection of ports to monitor while still providing sufficient coverage to detect many intruder scans. The **Standard** option extends this coverage by introducing additional monitored ports for early detection of intruder scans. The **Strict** button installs a comprehensive selection of ports to monitor and should be sufficient to detect most scans.

Warning

The list of network ports can be freely edited, however adding network ports used by services running on the SG unit (such as telnet) may compromise the security of the device and your network. It is strongly recommended that you use the pre-defined lists of network ports only.

Advanced Intrusion Detection and Prevention (Snort and IPS)

Advanced Intrusion Detection and Prevention is based on two variants of the tried and tested intrusion detection and prevention system Snort v2.

Snort in IDS (Intrusion Detection System) mode resides in front of the firewall, and detects and logs a very wide range of attacks. Snort in IPS (Intrusion Prevention System) mode resides behind the firewall, and detects and blocks a wide range of attacks.

The primary advantage of running Snort IDS (**Snort**) in front of the firewall is that it sees unfiltered network traffic, and therefore be able to detect a wider range of attacks. The primary advantage of running Snort IPS (**IPS**) behind the firewall is that suspicious network traffic can be disallowed, rather than simply flagged as suspicious and allowed and pass.

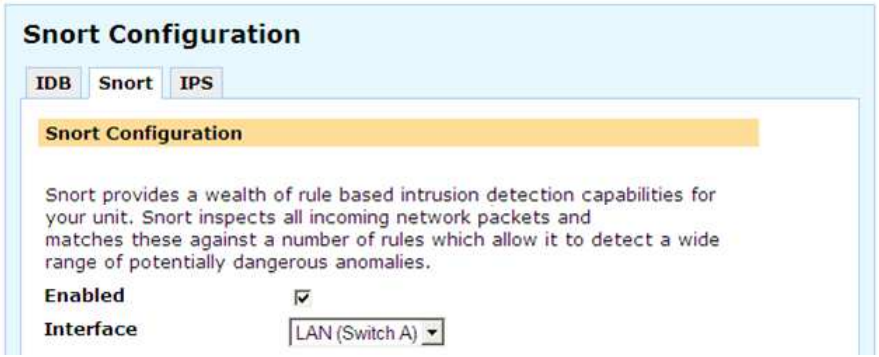
Snort uses a combination of methods to perform extensive network traffic analysis on the fly. These include protocol analysis, inconsistency detection, historical analysis and rule based inspection engines. Snort can detect many attacks by checking destination port number, TCP flags and doing a simple search through the packet's data payload. Rules can be quite complex, allowing a trigger if one criterion matches but another fails and so on. Snort can also detect malformed network packets and protocol anomalies.

Snort can detect attacks and probes such as buffer overflows, stealth port scans, CGI attacks, NetBIOS SMB probes, OS finger printing attempts and many other common and not so common exploits.

You may use Snort is IDS and IPS mode simultaneously if you choose, however it consumes a lot of the SG unit's memory.

Snort and IPS configuration

Select **Intrusion Detection** from the **Firewall** section of the main menu, and click the **Snort** tab to configure Snort in IDS mode, or **IPS** to configure Snort in IPS mode. The fields displayed


Snort Configuration
IDB
Snort
IPS
Snort Configuration
Snort provides a wealth of rule based intrusion detection capabilities for your unit. Snort inspects all incoming network packets and matches these against a number of rules which allow it to detect a wide range of potentially dangerous anomalies.
Enabled
Interface
LAN (Switch A)

Check **Enabled.**

Select the network **Interface** to monitor (*Snort IDS only*). This is typically **Internet**, or possibly **DMZ**.

Check **Use less memory** to restrict Snort's memory usage (*Snort IPS only*). This results in slower signature detection throughput, but may be necessary if the device is configured to run many services, many VPN tunnels, or both Snort IDS and IPS.

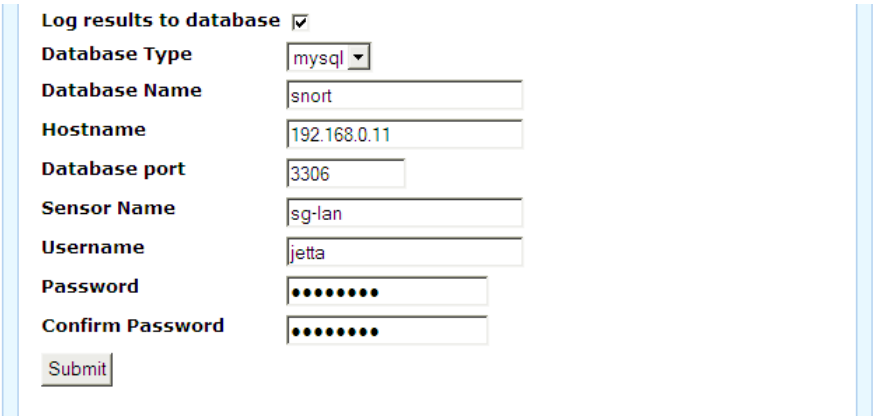
Rule sets are sets of defined patterns or rules used for the detection of attacks. These are grouped by type such as **ddos**, **exploit**, **backdoor**, **netbios**, etc. Each group encompasses many attack signatures. The full list of signatures can be viewed at the Snort web site (http://www.snort.org).

Note

The more rule sets that are selected, the greater load is imposed on the device. Therefore a conservative rather than aggressive approach to adding rule sets should be followed initially.

Logging to an analysis server (Snort IDS only)

Typically, Snort in IDS mode is configured to log intrusion attempts to a remote database server, which in turn runs an analysis console. An analysis console, such as BASE (Basic Analysis and Security Engine), is an application purpose built for analyzing this log output.



Log results to database to use a remote analysis server. If it is left unchecked, results are output to the device's system log (**Advanced** -> **System Log**).

The device currently only supports the *MySQL* **Database Type**.

Enter the table name of remote data in **Database Name**.

Enter the IP address or resolvable **Hostname** of the analysis server.

Enter the **Database port** of the analysis server. For MySQL type databases, this is typically 3306.

Sensor Name is an arbitrary string that is prepended to the log output. This may be useful if you have deployed more than one intrusion detection system.

Enter the **Username** and **Password** required for authentication to the remote database.

Click **Submit** to apply your changes.

Setting up the analysis server

Specific open source tools are required to be installed on the Analysis server for a straightforward evaluation.

The analysis server is typically a Pentium 4 level system running Linux (*Red Hat*, *Debian*, etc.) with sufficient memory and disk capacity to run a database and web server with at least one Ethernet port. With these tools installed, web pages can be created that display, analyze and graph data stored in the MySQL database from the SG unit running Advanced Instrusion Detection. They should be installed in the following order:

MySQL database

http://www.mysql.com/downloads/mysql-4.0.html

http://www.mysql.com/doc/en/index.html

Apache web server

http://httpd.apache.org/download.cgi

http://httpd.apache.org/docs-2.0/

PHP scripting language for developing web pages

http://www.php.net/downloads.php

http://www.php.net/download-docs.php

ADODB library to hide differences between databases used by PHP

http://php.weblogs.com/adodb#downloads

GD graphics library for GIF image creation used by PHP

http://www.boutell.com/gd/

PHPlot graph library for charts written in PHP

http://www.phplot.com/

BASE analysis console

http://secureideas.sourceforge.net/

Snort is running as an IDS sensor on the SG unit, logging to the MySQL database on the analysis server. The *Downloads* section of the BASE website contains detailed documents that aid in installing the above tools on the analysis server.

Access Control and Content Filtering

The access control web proxy allows you to control access to the Internet based on the type of web content being accessed (**Content** or **Webwasher**), and which user or workstation is accessing the Internet content (**Require user authentication**, **IP Lists**). This is useful to minimize inappropriate Internet use.

Additionally, you can set up global block/allow lists for web sites that you always want to be accessible/inaccessible (**Web Lists**), or force users to have a personal firewall installed (**ZoneAlarm**) or ensure they are not running network services that may be exploited (**Policy**) before accessing the Internet.

How access controls are applied

Access control options operate in the following order for web access:

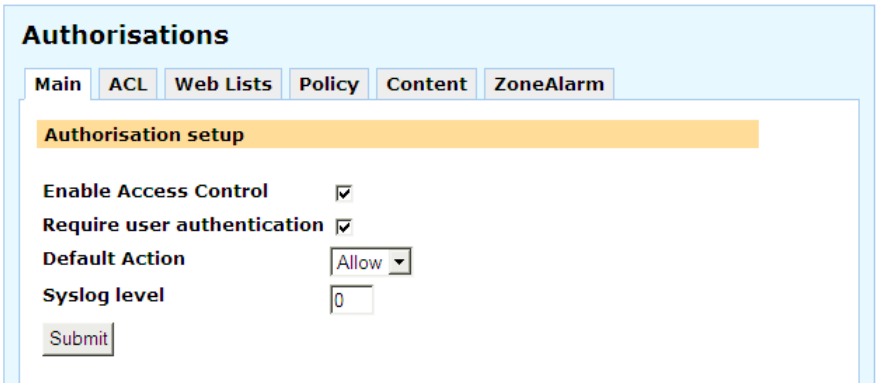
1. **Web Lists** allow
2. **Web Lists** deny
3. Security **Policy** enforcement
4. **ACL** allow
5. **ACL** block
6. **ZoneAlarm**
7. Content filtering (**Content** or **Webwasher**)

Access control options operate in the following order for all other Internet access:

1. Security **Policy** enforcement
2. **ACL** allow
3. **ACL** block
4. **ZoneAlarm**

Enabling access control

Select **Access Control** from the main menu, then the **Main** tab.



The **Enable Access Control** checkbox enables/disables the entire access control subsystem. This box must be checked for *any* access control operation to take place.

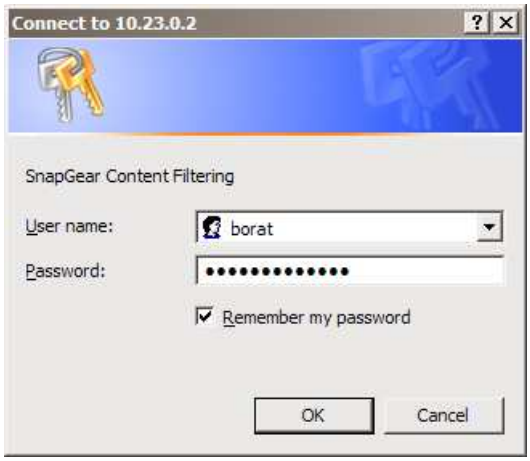
The **Default Action** field defines the behaviour when none of the myriad of settings positively allow or block access. If changed to *block by default*, some definitions must be created elsewhere in access control to allow some network traffic or no access is possible.

The **Require user authentication** checkbox determines if users are asked for a username and password when attempting to access the web through the SG unit.

The **Syslog level** controls the level of debug output that is logged to the system log. The higher this is set to, the more verbose the output. For normal operation, this should be set to **0** or very large logs and a noticable system slow down might result. For normal debugging, set this to **1**. Higher levels need only be turn on when so directed by Secure Computing support.

User authentication

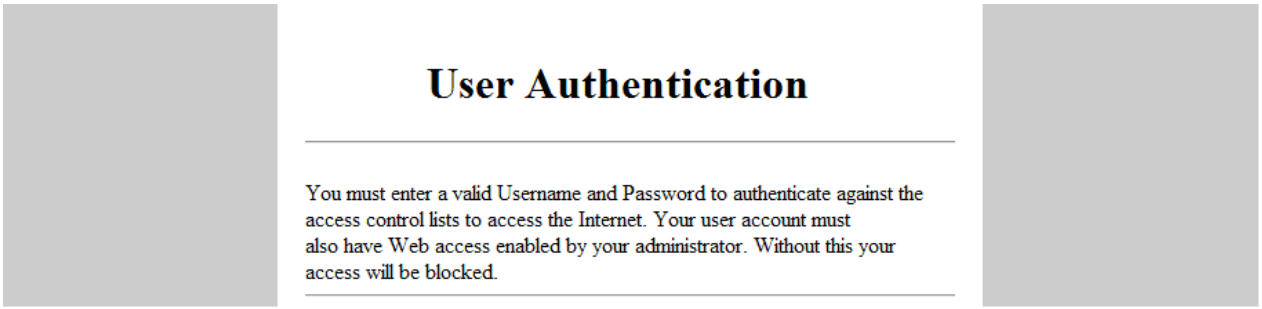
Check **Require user authentication** if you want to require users to authenticate themselves before browsing the web. When attempting to access a web site on the Internet, their browser displays a dialog similar to the following:



Note

To add or remove access controls user accounts, select ***Users*** *from the main menu and click the* ***Local Users*** *tab. Access controls users should generally have only* ***Internet Access (via. Access Controls)*** *checked, with all other access permissions unchecked. See the* Users *section in the chapter entitled* System *for further details on adding user accounts.*

Users without web proxy access see a screen similar to the figure below when attempting to access external web content.


User Authentication
You must enter a valid Username and Password to authenticate against the access control lists to access the Internet. Your user account must also have Web access enabled by your administrator. Without this your access will be blocked.

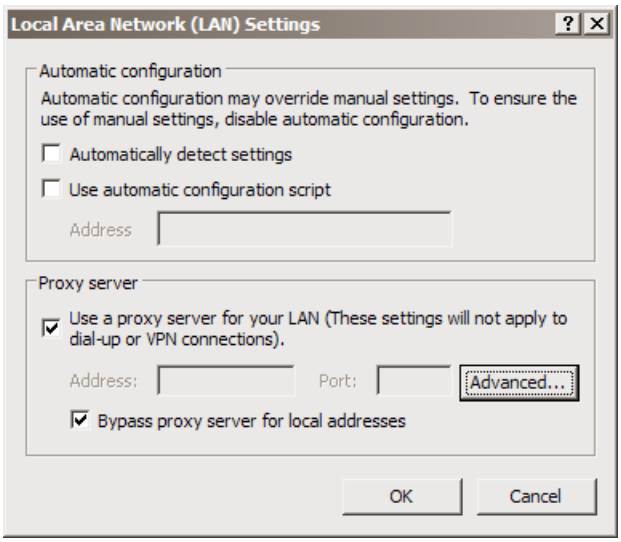
Note

Each browser on the LAN now has to be set up to use the SG unit's web proxy.

Browser setup

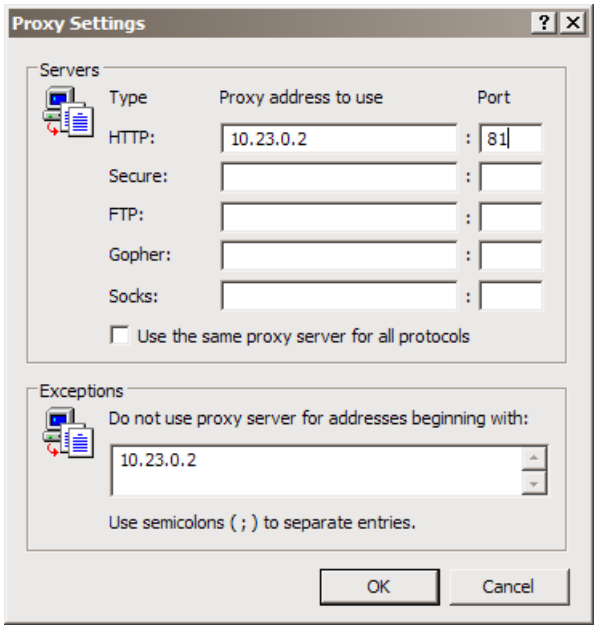
The example given is for Microsoft Internet Explorer 6. Instructions for other browsers should be similar, refer to their user documentation for details on using a web proxy.

From the **Internet Options** menu, select **Tools**. From the **LAN Settings** tab, select **LAN Settings**.


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
Port:
Advanced...
Bypass proxy server for local addresses
OK
Cancel

Check **Use a proxy server for your LAN…** and **Bypass proxy server for local address**. All other options should remain unchecked.

Click **Advanced**.



In the row labeled **HTTP**, enter your SG unit's LAN IP address in the **Proxy address to use** column, and *81* in the **Port** column. Leave the other rows blank.

In the **Exceptions** text box, enter your SG unit's LAN IP address.

Click **OK**, **OK** and **OK** again.

ACL

Access may be **Block**ed or **Allow**ed by the **Source** (LAN) IP address or address range, the **Destination** (Internet) host's IP address or address range, or the **Destination Host**'s name.

Addresses are added through **Definitions** -> **Addresses**, refer to the *Definitions* section earlier in this chapter for further detail.

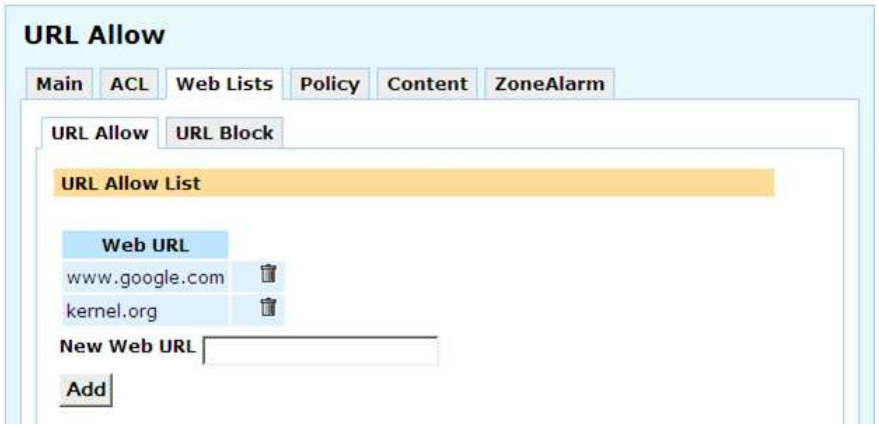
Note

*All Internet traffic, not just web traffic, is affected by **ACL**.*

Web lists

Access is be denied to any web address (URL) that contains text **Add**ed under **URL Block List**, e.g. entering *xxx* blocks access to any URL containing *xxx*, e.g.: http://www.xxx.com, http://xxx.example.com or www.test.com/xxx/index.html

The **Allow List** also enables access to URLs containing the specified text.



Note

Defining large numbers of URL fragments to match against can result in a significant slowing down of WWW accesses. Defining overly short URL fragments can result in many sites matching and being allowed or denied erronously.

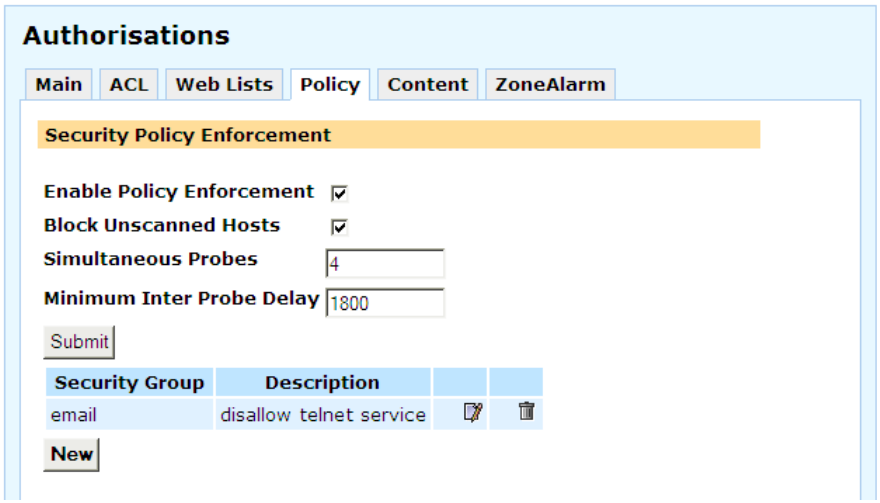
Policy

This access control module allows a site's security policy to be partially actively enforced. Hosts which do not adhere to their defined policy are automatically denied access through the firewall.

A number of **Security Groups** can be defined where each group contains a number of host IP addresses or IP address ranges. Each group is aditionally given a number of permitted and denied services which they are allowed to offer. Each host in each group are periodically actively scanned for the services they are not allowed to offer and if a connection to one of these services is successful, the host is black listed until such time as the offending service is no longer offered. Scans are never performed against permitted services. A number of predefined allow and deny service lists are provided, however, these should really be considered a guideline only as they are not a replacement for a well thought out and designed security policy.

In addition to enforcing the services aspect of security groups, it is possible to include a number of NASL (*Nessus Attack Scripting Language*) scripts in */etc/config* on the unit and to define some or all of these to be run against the target hosts. Typically, one would use attack scripts from the Nessus suite to scan for specific vulnerabilities and exploits on a host. If any script detects such a vulnerability, Internet access is again blocked. The list of available scripts is automatically populated from the files ending with *.nasl* in */etc/config*.

Security groups may overlap with respect to hosts within them. In this case, a single allow service overrides any number of denies of that same service. However, NASL scripts and overlapping groups do not interoperate particularly and should be avoided.



The top level page has a checkbox **Block Unscanned Hosts** which defines the behaviour for a host which hasn't been scanned or is not defined to be scanned.

The **Minimum Inter Probe Delay** specifies a minimum number of seconds between scans of a single host. It also specifies the maximum time for changes to take effect.

The **Simultaneous Probes** setting specifies the maximum number of different hosts that should be scanned together.

Content filtering

Note

Content filtering is only available after your have registered your SG unit and activated your content filtering licence (sold separately). See the Obtaining a content filtering licence *section below.*

Content filtering allows you to limit the types of web based content accessed.

Note

*Content filtering is not performed for addresses specified in **Web Lists** or **ACL**.*

Obtaining a content filtering licence

Contact your local SG dealer to obtain a content filtering licence.

When you purchase a content filtering licence, you are given a token to activate the licence. Navigate to http://www.cyberguard.com/snapgear/my/ and ensure the unit on which you want to run content filtering is registered; if not, register it now using **Quick product registration**. Enter the token in **Quick addon activation** and associate the licence with the registered unit.

Your licence key or certificate and private key and now available by clicking **List registered units and options**, then clicking the **View URL filter data** for the appropriate unit.

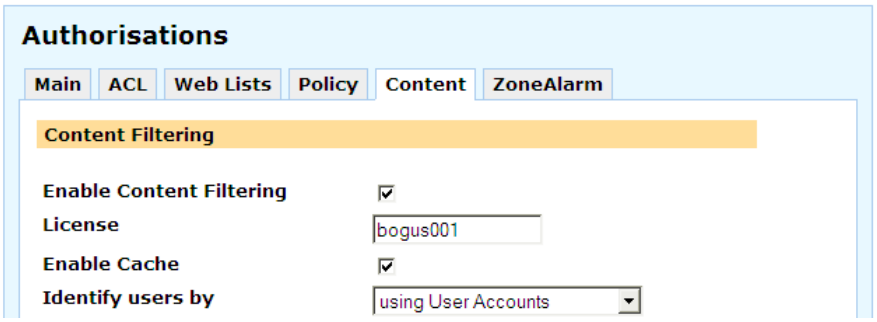
Content or Webwasher?

Webwasher is Secure Computing's next generation of content filtering. In time, the original content filtering system (**Content**) will be phased out. Webwasher offers more categories for rating, and operates significantly faster than the old system.

All new content filtering subscriptions are for the Webwasher service. The old content filtering system is maintained for backwards compatibility for existing subscribers only.

If you have been given a single licence key, you have a subscription to the original **Content** system. If you have been given a certificate and private key, you have a subscription to the new **Webwasher** system.

Content



Check **Enable Content Filtering** enter your **License key** then continue on to set reporting options and which categories to block. Click **Apply** once these options have been set up to enable content filtering.

Checking **Enable Cache** stores recently accessed pages' ratings locally, to lower the response time the next time the page is accessed. It is recommended that you leave this checked.

Blocked requests are submitted to the central content filtering server. The user attempting to access blocked content can be identified either through **User Accounts** (see *User Authentication earlier* in this chapter) or the IP **Address of their machine**.

Click the **Reports** tab to connect to the central content filtering server. Enter your **Customer ID**, **Username** and **Password** that were issued with your content filtering license. Click **View Reports**.

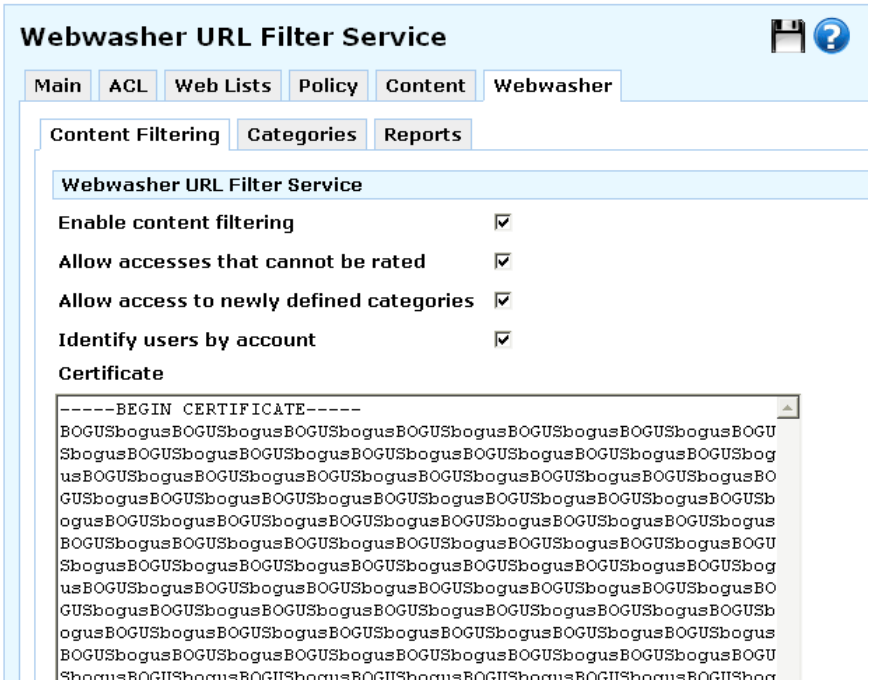
Warning

The correct time/date must be set on your SG unit for reporting to work. The most effective way to do this is by using an NTP time server. See the Time and Date *section in the chapter entitled* System *for details.*

Also note that the username and password is not the same as the one used to access your SG unit, check http://www.cyberguard.com/snapgear/my/ for login details.

Select which categories you wish to block. Selecting **Unratable** blocks pages that the central content filtering database has not yet categorized.

Webwasher



Check **Enable content filtering** and paste in your **Certificate** and **Private key**.

Check **Allow accesses that cannot be rated** to allow access to web sites that the Webwasher content filtering system has not yet rated. The default behaviour is to block all unrated sites.

The SG unit dynamically retrieves rating categories from the Webwasher server. As such, new categories may be added after content filtering is configured on your SG unit.

Unchecking **Allow access to newly defined categories** restricts access to the categories you did not block when configuring content filtering. Leaving **Allow access to newly defined categories** checked allows access to any categories added after content filtering is configured.

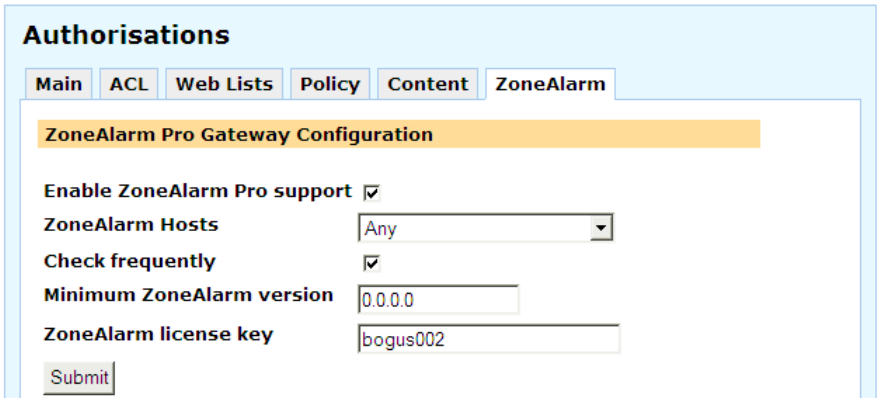
Check **Identify users by account** to send user names to the Webwasher reporting service. In order for this field to have any effect, **Require User Authentication** on the **Main** tab must be checked.

Under the **Categories** tab, select the **Blocked Categories** to block access to.

Under the **Reports** tab, enter your **Username** and **Password** and click **View Reports** to view reporting on blocked accesses, etc.

ZoneAlarm

The ZoneAlarm Pro section of access control allows for the blocking of local hosts which aren't running ZoneAlarm Pro software or which aren't running a sufficiently recent version of ZoneAlarm Pro software. ZoneAlarm Pro provides a measure of protection against malware for hosts and being able to allow Internet access based on this protection being present and operational can be useful.



The **Enable ZoneAlarm Pro support** checkbox specifies if the ZoneAlarm Pro enforcement section of access control is active or not. Turning this feature on does involve a small sacrifice in the performance of this unit.

The **ZoneAlarm Hosts** menu allows selection of the hosts which must be running ZoneAlarm Pro software to be able to access the Internet.

The **Check frequently** checkbox indicates if local hosts should be queried as to their ZoneAlarm Pro status and version very often or less often. Turning this on involves a small sacrifice in the performance of this unit and a slight increase in network activity.

The **ZoneAlarm licence key** must contain a valid ZoneAlarm Pro licence or this section of access control is inoperative. Licences are available from ZoneLabs.

Antivirus

Note

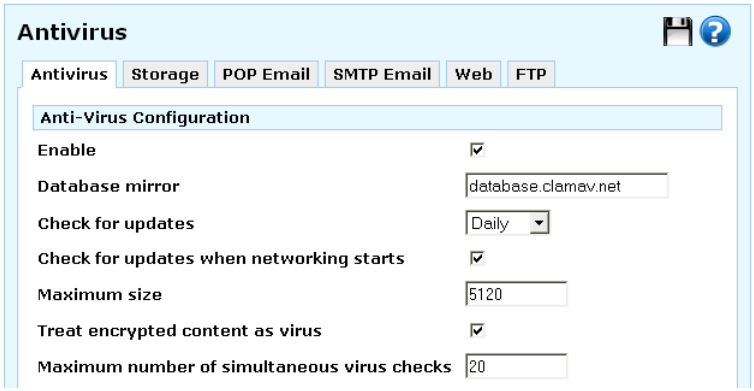
SG565, SG580 and SG710 only.

The SG unit's antivirus capabilities shield your LAN from viruses that propagate through email, the web and FTP. An antivirus subscription is not required and virus definitions are automatically kept up-to-date.

The SG unit is equipped with proxies for POP, SMTP, HTTP and FTP that facilitate the transparent scanning of files passing through it. If a virus is detected, the user on your LAN sending or receiving the infected file or email is informed by an error message or error email, and the infected file or email is not delivered to its destination.

Enable antivirus

Select **Antivirus** from the **Firewall** section of the main menu.



Check **Enable**.

The **Database mirror** is the host from which the signature database is updated. Unless there is a specific host from which you want the SG unit to retrieve signature updates, leave this at the default setting of *database.clamav.net*.

Select the frequency to **Check for updates** from the database mirror. The checks are quick and shouldn't cause a noticeable decrease to performance unless an update is necessary.

Enable **Check for updates when networking starts** to force a virus signature update when the status of the network changes, e.g. when the Internet connection comes online. This guarantees a virus signature update when the SG units boots.

Specify the **Maximum size** in kilobytes of files to scan for viruses. Files over this size are automatically rejected.

You may **Treat encrypted content as virus**es – as the SG unit is not the intended receipient, it does not decrypt encrypted content passing through it, and cannot determine whether such content is infected.

Specify the **Maximum number of simultaneous virus checks** to perform. Permitting more scans increases the amount of memory and CPU resources required by the antivirus scanning.

Click **Submit**.

Storage

It is recommended that you use a network or local share to provide storage for the virus database and temporary space for the scanning process. This greatly increases the effectiveness of the antivirus scanner.

Network storage

A network share is a shared folder or drive on a local Windows PC, or a PC running another operating system capable of SMB sharing (such as Mac OS X, or a Linux PC running the SAMBA service).

Refer to your operating system's documentation for details on creating a network share. What follows are some basic instructions for creating a network share under Windows XP.

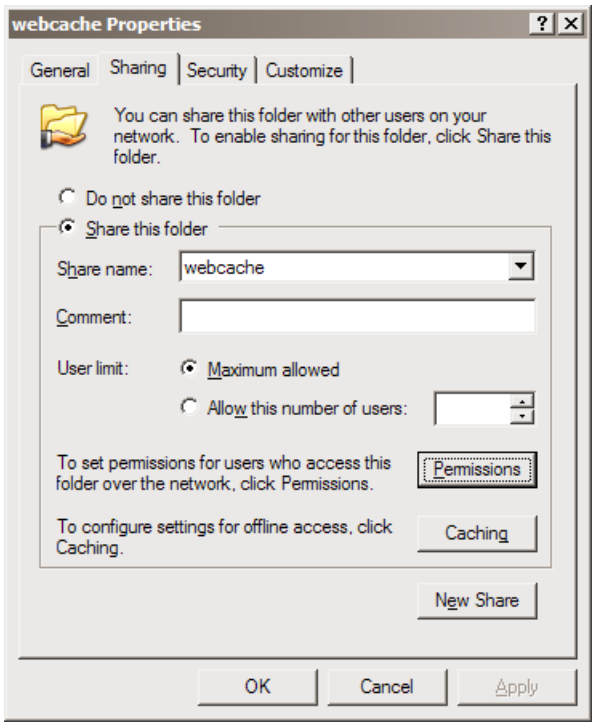
- Create a new user account:

Note

We recommend that you create a special user account to be used by the SG unit for reading and writing to the network share. If you have an existing account or wish to may the network share readable and writeable by everyone, you may skip the next step.

To create an account, click **Start** -> **Control Panel** -> **User Accounts** -> **Create a new account**. Type a name for the new account, e.g. *sguser*, and click **Next**. Typically it is sufficient to grant this account **Limited** privileges. Click **Create Account** to create it. Select the account you have just create under **Pick an account to change**. Select **Create a password**. Enter and confirm a password for this account, as well as a password hint if desired.

- Create the network share:



Launch Windows Explorer (**Start** -> **(All) Programs** -> **Accessories** -> **Windows Explorer**) and open up a folder or drive to dedicate as a network share for use by the SG unit's web cache.

Begin by disabling simple file sharing for this folder. From the **Tools** menu, select **Folder Options**. Click the **View** tab and under the **Advanced settings** section *uncheck* **Use simple file sharing (Recommended)**. Click **OK**.

Next, share the folder. Right click on the folder and select **Sharing and Security**. Select **Share this folder** and note the **Share name**, you may change this to something easier to remember if you wish.

Finally, to set the security permissions of the newly created network share, click **Permissions**.

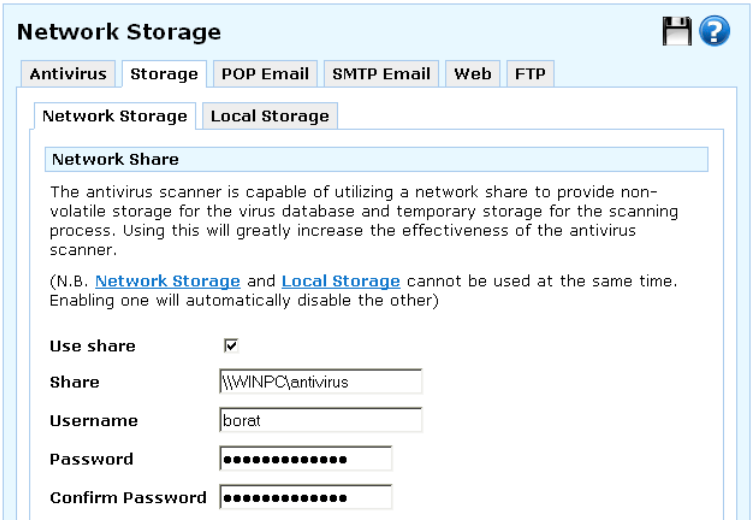
If you wish to secure the network share with a username and password (recommended), click **Add** and type the user name the account to be used by the SG unit and click **Check Names** then **OK**.

Select this account, or **Everyone** if you are not securing the network share with a username and password, and check **Allow** next to **Full Control**. Click **OK** and **OK** again to finish.

- Set the SG unit to use the network share

Under the **Storage** -> **Network Storage** tab, check **Use share**. Enter the location of the network share in the format:

\\HOSTNAME\sharename


Network Storage
Antivirus
Storage
POP Email
SMTP Email
Web
FTP
Network Storage
Local Storage
Network Share
The antivirus scanner is capable of utilizing a network share to provide non-volatile storage for the virus database and temporary storage for the scanning process. Using this will greatly increase the effectiveness of the antivirus scanner.
(N.B. Network Storage and Local Storage cannot be used at the same time. Enabling one will automatically disable the other)
Use share
Share
\\WINPC\antivirus
Username
borat
Password
Confirm Password

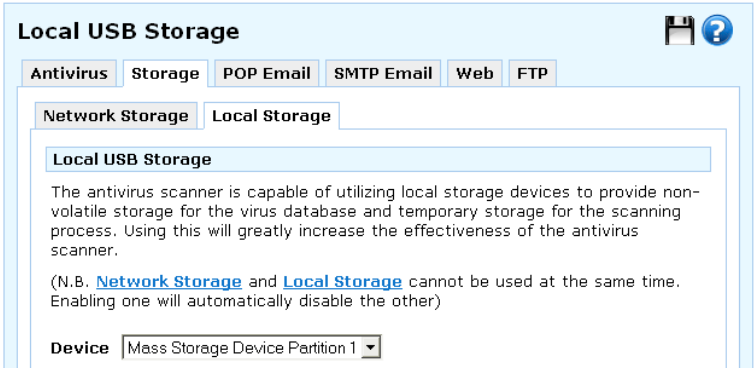
Enter the **Username** and **Password** for a user that can read and write to the network share. If you allowed **Full Control** to **Everyone**, you may leave these blank.

Local storage

Note

SG565 only.

Attach a USB storage device to one of the SG unit's USB ports.


Local USB Storage
Antivirus
Storage
POP Email
SMTP Email
Web
FTP
Network Storage
Local Storage
Local USB Storage
The antivirus scanner is capable of utilizing local storage devices to provide non-volatile storage for the virus database and temporary storage for the scanning process. Using this will greatly increase the effectiveness of the antivirus scanner.
(N.B. Network Storage and Local Storage cannot be used at the same time. Enabling one will automatically disable the other)
Device
Mass Storage Device Partition 1

Under the **Storage** -> **Local Storage** tab, select the partition or device to use from the **Device** pull down menu, and click **Submit**.

POP email

The SG unit can scan email being sent by PCs on your LAN before delivering it to the destination mail server.

Note

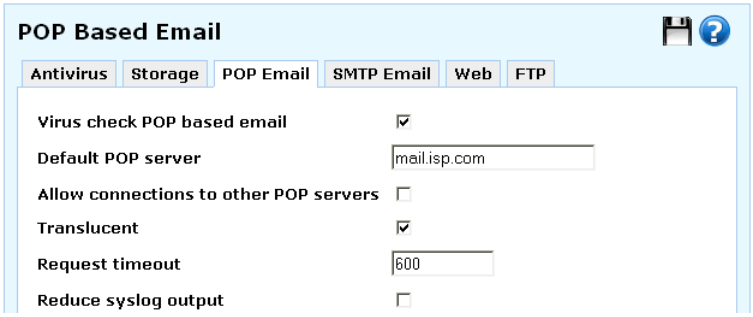
Scanning of IMAP and web-based email is not supported.

This service is configured differently depending on whether you want to scan all incoming email, or email being retrieved by specific PCs on your LAN only.

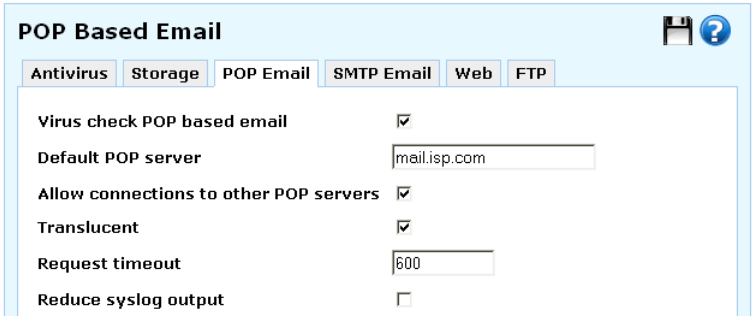
Scan all POP email

Check **Virus check POP based email**.

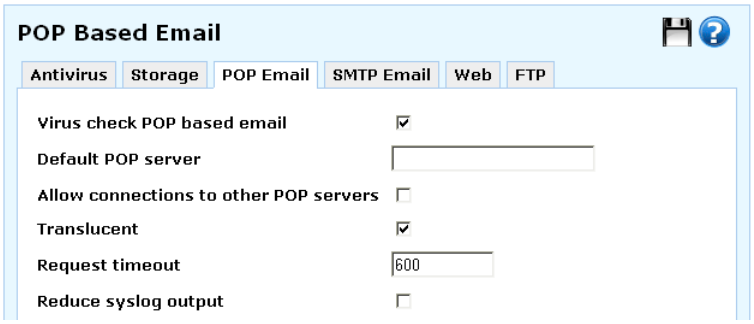
Check **Translucent**.



If all of your internal email clients (such as Microsoft Outlook) are retrieving email from a single mail server only, enter it as the **Default POP server**. Uncheck **Allow connections to other POP servers**.



If most, but not all, of your internal email clients are retrieving email from a single mail server, enter this as the **Default POP server**. Check **Allow connections to other POP servers**.



If there is no single mail server from which most of your internal email clients are retrieving email, leave **Default POP server** blank and check **Allow connections to other POP servers**.

Note

For each of the email clients that is not retrieving email from the default POP server (this may be all email clients), the email client's POP (or POP3) username setting must be in the form of user@mail.isp.com*, rather than simply* user – user *is the POP login, and* mail.isp.com *is the POP mail server.*

Typically it is not necessary to adjust the POP protocol **Request timeout**.

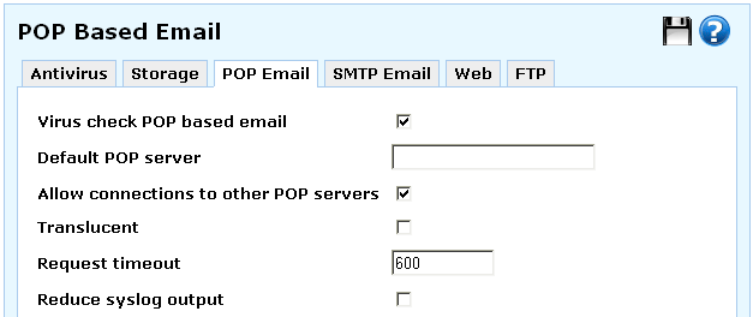
Once POP scanning is functioning properly, you may choose to **Reduce syslog output**.

Click **Submit**.

Scan POP email for specific clients only

Check **Virus check POP based email**.

Uncheck **Translucent**.



Leave **Default POP server** blank and check **Allow connections to other POP servers.**

Note

For each of the email clients for which to scan incoming mail, the email client's POP3 username setting must be in the form of user@mail.isp.com*, rather than simply* user *–* user *is the POP3 login, and* mail.isp.com *is the POP3 mail server.*

Additionally, the email client's incoming/POP3 email server setting must be sent to the SG unit's LAN IP address (e.g. 192.168.0.1).

Typically it is not necessary to adjust the POP3 protocol **Request timeout**.

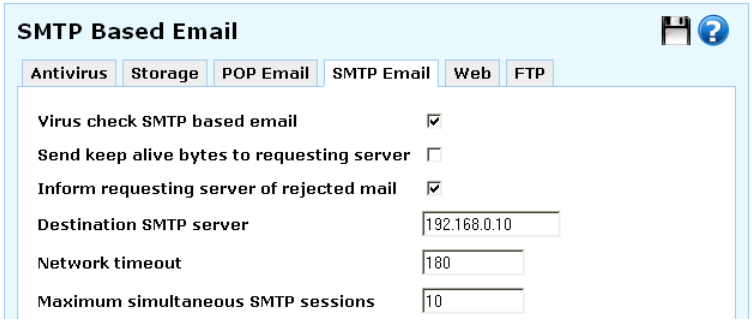
Once POP3 scanning is functioning properly, you may choose to **Reduce syslog output**.

Click **Submit**.

SMTP email

If you have an SMTP mail server on your LAN, the SG can scan emails sent to it by external mail servers.

Check **Virus check SMTP based email**.



Enter your LAN's SMTP mail server address as the **Destination SMTP server**.

Check **Send keep alive bytes to requesting server** to send keep alive traffic to the source SMTP server. This option is only useful on slow network connections where the source server is timing out before the SG unit has finished its virus checking.

When **Inform requesting server of rejected mail** is enabled the SG unit rejects incoming mail that is detected to have a virus, and informs the requesting SMTP server that the mail has been dropped. This is the default and recommended behaviour.

When **Inform requesting server of rejected mail** is disabled the SG unit accepts and then subsequently drops incoming mail that is detected to contain a virus. The requesting mail server believes the mail was delivered correctly, however the SG unit drops the mail without a notification being sent to either the sender of the mail or the requesting server.

Typically, the default **Network timeout** for this is appropriate and should only be changed if there are time out problems.

You may specify the **Maximum simultaneous SMTP sessions** to set the maximum number of simultaneous SMTP connections. Increasing this increases the resources consumed by virus scanning.

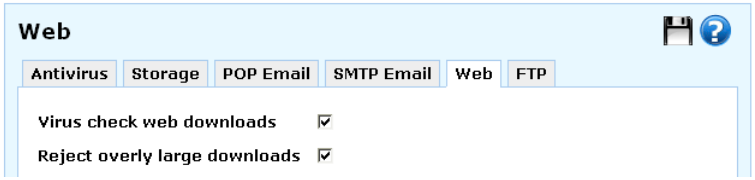
Click **Submit**.

Web

The SG unit can scan incoming web traffic for viruses.

Note

*Enabling this automatically enables **Access Control**.*



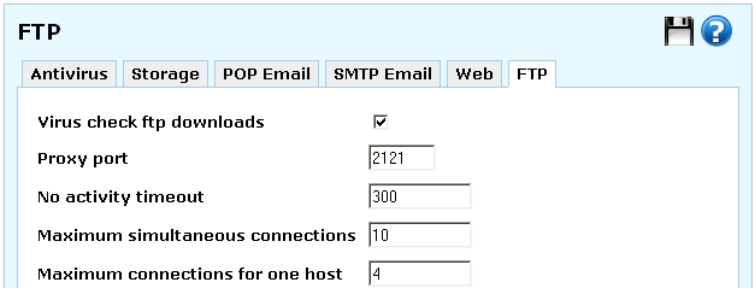
Check **Virus check web downloads**.

Check **Reject overly large downloads** to have the SG unit treat oversized downloads as potential viruses and reject them. The definition of an *overly large download* is specified by the **Maximum size** field on the main **Antivirus** tab.

Click **Submit**.

FTP

The SG unit can scan files downloaded using FTP for viruses.



Check **Virus check FTP downloads**.

Typically there is no need to change the **Proxy port** on which the transparent proxy listens for connections.

If an FTP connection is idle for the number of seconds specified by **No activity timeout**, it is automatically disconnected. Increase this only if you are experiencing timeouts during FTP sessions.

You may specify the **Maximum simultaneous connections** to allow. This is the total number of FTP connections allowed from your LAN. Once this number is reached, subsequent FTP connections are rejected until previous FTP connections are disconnected. More resources are consumed by virus scanning when a higher number of simultaneous FTP connections are established.

You may specify the **Maximum connections for one host** to allow. This is the number of FTP connections allowed from a single PC. Once this number is reached, subsequent FTP connections are rejected until previous FTP connections are disconnected.

Click **Submit**.

5. Virtual Private Networking

Virtual Private Networking (VPN) enables two or more locations to communicate securely and effectively, usually across a public network (e.g. the Internet) and has the following key traits:

- **Privacy** - no one else can see what you are communicating
- **Authentication** - you know who you are communicating with
- **Integrity** - no one else can tamper with your messages/data

Using VPN, you can access the office network securely across the Internet using Point-to-Point Tunneling Protocol (PPTP), IPSec or L2TP. If you take your portable computer on a business trip, you can dial a local number to connect to your Internet access provider and then create a second connection (called a *tunnel*) into your office network across the Internet and have the same access to your corporate network as if you were connected directly from your office. Similarly, telecommuters can also set up a VPN tunnel over their cable modem or DSL links to their local ISP.

VPN technology can also be deployed as a low cost way of securely linking two or more networks, such as a headquarters LAN to the branch office(s). IPSec is generally the most suitable choice in this scenario.

With the SG unit you can establish a VPN tunnel over the Internet using either PPTP, IPSec or L2TP. IPSec provides enterprise-grade security, and is generally used for connecting two or more networks, such as a branch office to a head office.

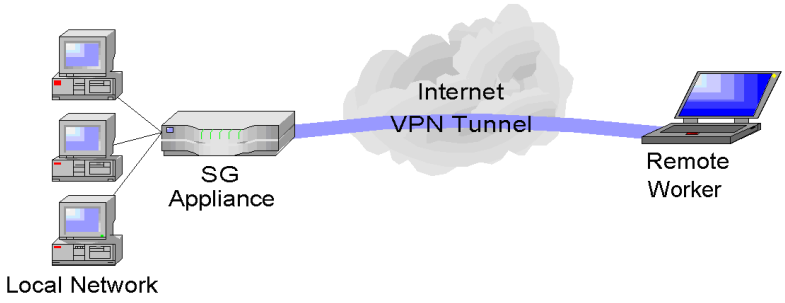
PPTP's strength is its ease of configuration and integration into existing Microsoft infrastructure. It is generally used for connecting single remote Windows clients.

L2TP combines elements of IPSec and PPTP. It is generally used as a relatively easy to configure way to bolster a PPTP-style connection from a remote Windows XP client with IPSec security.

This chapter details how to configure the L2TP and PPTP servers and clients, how to configure a remote client to connect, how to establish an IPSec tunnel, and also provides an overview of L2TP VPN tunneling.

PPTP and L2TP

The SG unit includes a PPTP and an L2TP VPN server. These allow remote Windows clients to securely connect to the local network.



PPTP or L2TP are also commonly used to secure connections from a Guest network; see the *Guest Network* section in the chapter entitled *Network Setup*.

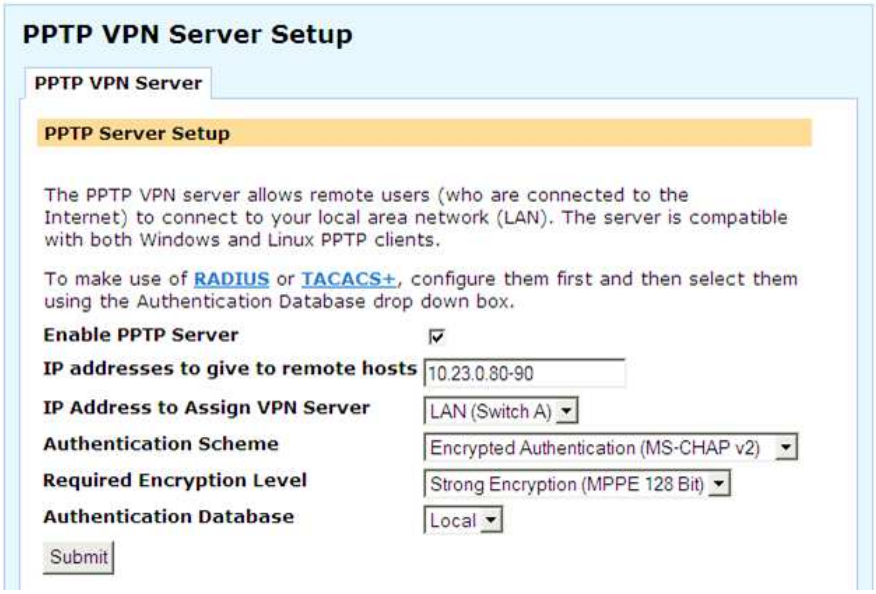
PPTP VPN Server

To setup a PPTP connection from a remote Windows client to your SG unit and local network:

- Enable and configure the PPTP VPN server.
- Set up VPN user accounts on the SG unit and enable the appropriate authentication security.
- Configure the VPN clients at the remote sites. The client does not require special software, the SG PPTP Server supports the standard PPTP client software included with Windows 95/98, Windows ME, Windows XP, WinNT and Windows 2000. The SG PPTP server is also compatible with Unix PPTP client software.
- Connect the remote VPN client.

Enable the PPTP server

Select **PPTP VPN Server** from the **VPN** section of the main menu.


PPTP VPN Server Setup
PPTP VPN Server
PPTP Server Setup
The PPTP VPN server allows remote users (who are connected to the Internet) to connect to your local area network (LAN). The server is compatible with both Windows and Linux PPTP clients.
To make use of RADIUS or TACACS+, configure them first and then select them using the Authentication Database drop down box.
Enable PPTP Server
IP addresses to give to remote hosts
10.23.0.80-90
IP Address to Assign VPN Server
LAN (Switch A)
Authentication Scheme
Encrypted Authentication (MS-CHAP v2)
Required Encryption Level
Strong Encryption (MPPE 128 Bit)
Authentication Database
Local
Submit

Check **Enable PPTP Server**.

Enter the **IP Addresses to give to remote hosts**, this must be a free IP address, or range of free IP addresses, from the network (typically the LAN) that the remote users are assigned while connected to the SG unit.

If you have configured several network connections, select the one that you want to connect remote users to from the **IP Address to Assign VPN Server** pull down menu. This is typically a LAN interface or alias.

Select the weakest **Authentication Scheme** to accept, access is denied to remote users attempting to connect using an authentication scheme weaker than this. They are described below, from strongest to weakest.

- **Encrypted Authentication (MS-CHAP v2):** The strongest type of authentication to use. This is the recommended option.
- **Encrypted Authentication (MS-CHAP):** This is not a recommended encryption type and should only be used for older dialin clients that do not support MS-CHAP v2.
- **Weakly Encrypted Authentication (CHAP):** This is the weakest type of encrypted password authentication to use. It is not recommended that clients connect using this as it provides very little password protection. Also note that clients connecting using CHAP are unable to encrypt traffic.
- **Unencrypted Authentication (PAP):** This is plain text password authentication. When using this type of authentication, the client passwords is transmitted un-encrypted.

Select the **Required Encryption Level**, access is denied to remote users attempting to connect not using this encryption level. Using **Strong Encryption (MPPE 128 Bit)** is recommended.

Select the **Authentication Database**. This allows you to indicate where the list of valid clients can be found. You can select from the following options:

- **Local:** Use the local database defined on the **Local Users** tab of the **Users** page. You must enable the **Dialin Access** option for the individual users that are allowed dialin access.
- **RADIUS:** Use an external RADIUS server as defined on the **RADIUS** tab of the **Users** page.
- **TACACS+:** Use an external TACACS+ server as defined on the **TACACS+** tab of the **Users** page.

Note

See the Users *section of the chapter entitled* System *for details on adding user accounts for PPTP access, and configuring the SG unit to enable authentication against a RADIUS or TACACS+ server.*

Add a PPTP user account

Select **Users** under **System** from the main menu, click **Local Users** and a **New** user with **PPTP Access**. Keep note of the **Username** and **Password**, as these are required in configuring the remote PPTP client.

Refer to the the *Users* section of the chapter entitled *System* for a more detailed account of adding a new local user.

Setup the remote PPTP client

To connect remote VPN clients to the local network, you need to know the username and password for the PPTP account you added, as well as the SG unit's Internet IP address.

Your Internet IP address is displayed on the **Network Setup** page. If your ISP has not allocated you a static IP address, consider using a dynamic DNS service. Otherwise you must modify the PPTP client configuration each time your Internet IP address changes. For details on configuring dynamic DNS, refer to the *DNS* section of the chapter entitled *Network Setup*.

Ensure the remote VPN client PC has Internet connectivity. To create a VPN connection across the Internet, you must set up two networking connections. One connection is for ISP, and the other connection is for the VPN tunnel to your office network.

Note

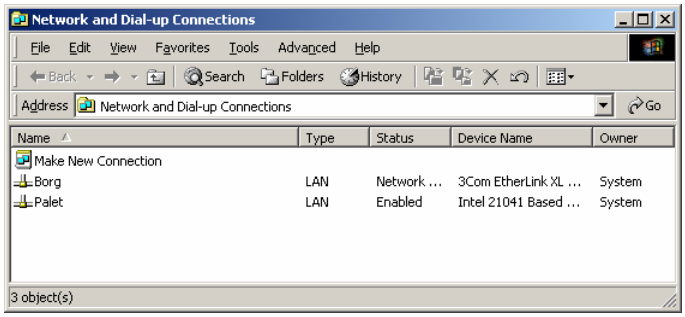
If you are using Windows 95 or an older version of Windows 98 (first edition), install the Microsoft DUN update *and* VPN Client update*, available from the Microsoft website.*

Your SG unit's PPTP server interoperates with the standard Windows PPTP clients in all current versions of Windows.

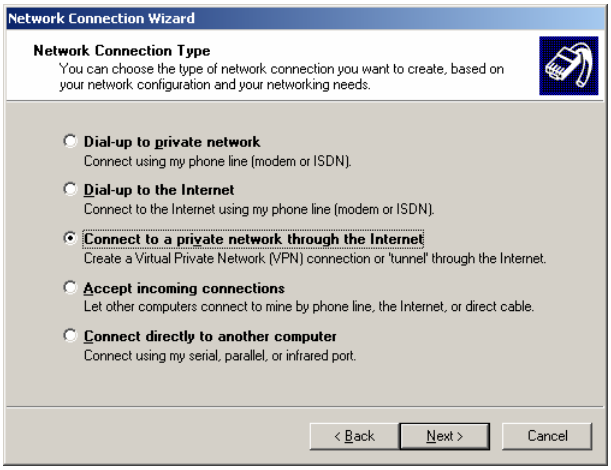
The following sections provide details for client setup in Windows 2000 and Windows XP. More detailed instructions are available in the Windows product documentation, and from the Microsoft website.

Windows 2000 PPTP client setup

Log in as *Administrator* or with Administrator privileges. From the **Start** menu, select **Settings** and then **Network and Dial-up Connections**. A window similar to the following is displayed.

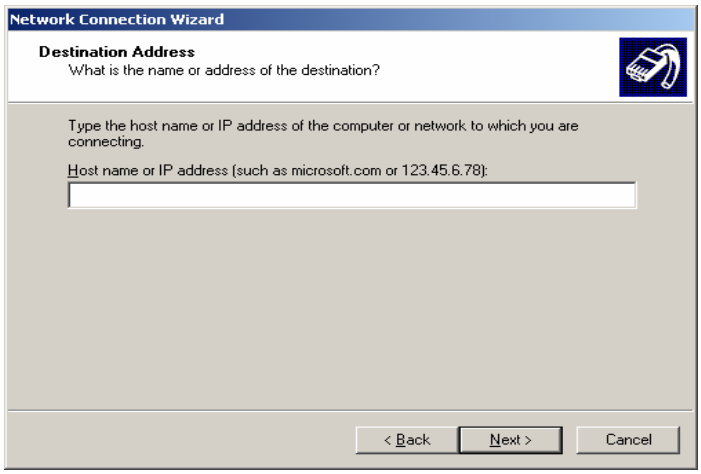

Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Name Type Status Device Name Owner
Make New Connection
Borg LAN Network ... 3Com EtherLink XL ... System
Palet LAN Enabled Intel 21041 Based ... System
3 object(s)

Double-click **Make New Connection** from the main windows. Click **Next** to show the **Network Connection Type** window:


Network Connection Wizard
Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.
Dial-up to private network
Connect using my phone line (modem or ISDN).
Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).
Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.
Connect directly to another computer
Connect using my serial, parallel, or infrared port.
< Back
Next >
Cancel

Select **Connect to a private network through the Internet** and click **Next**.

This displays the **Destination Address** window:


Network Connection Wizard
Destination Address
What is the name or address of the destination?
Type the host name or IP address of the computer or network to which you are connecting.
Host name or IP address (such as microsoft.com or 123.45.6.78):
< Back
Next >
Cancel

Enter the SG unit's Internet IP address or fully qualified domain name and click **Next**. Select the **Connection Availability** you require on the next window and click **Next** to display the final window:

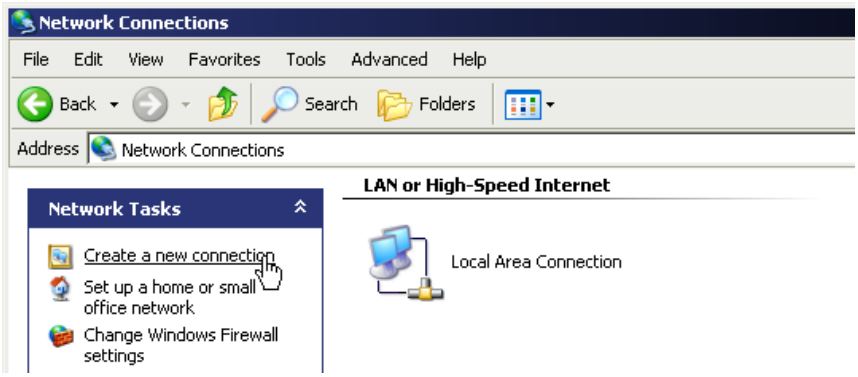
Network Connection Wizard
Completing the Network Connection Wizard
Type the name you want to use for this connection:
Virtual Private Connection
To create this connection and save it in the Network and Dial-up Connections folder, click Finish.
To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.
Add a shortcut to my desktop
< Back
Finish
Cancel

Enter an appropriate name for your connection and click **Finish**.

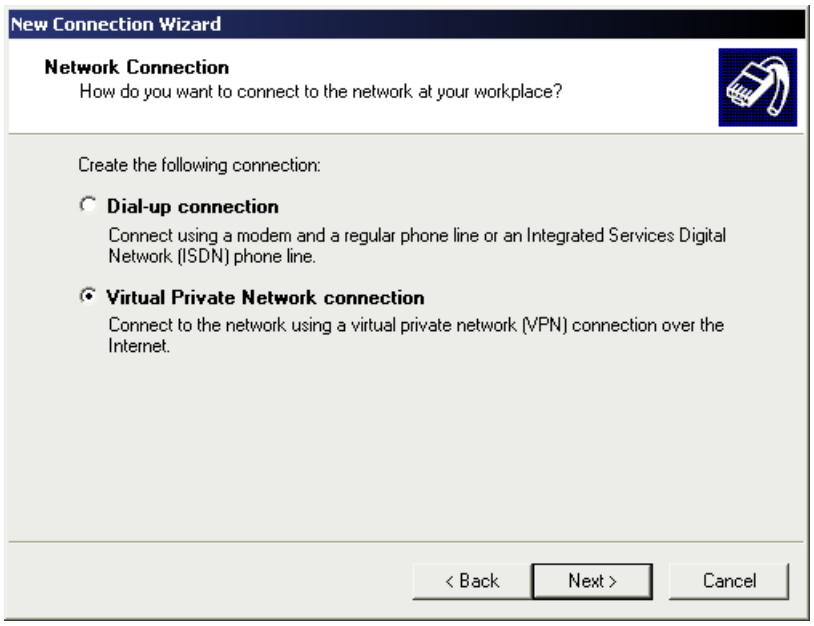
Your VPN client is now set up and ready to connect.

Windows XP PPTP client setup

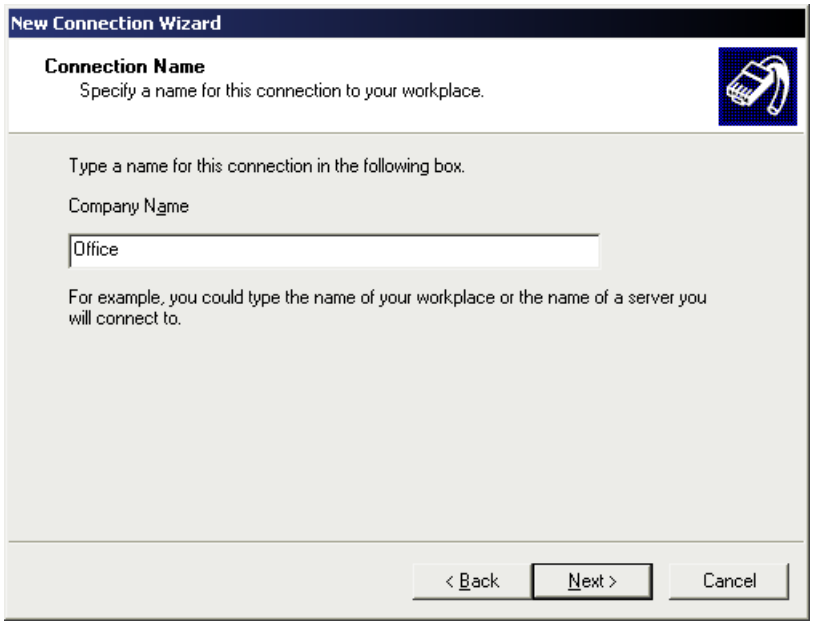
Log in as *Administrator* or with Administrator privileges. From the **Start** menu, select **Settings** and then **Network Connections**.



Click **Create New Connection** from the **Network Tasks** menu to the left.

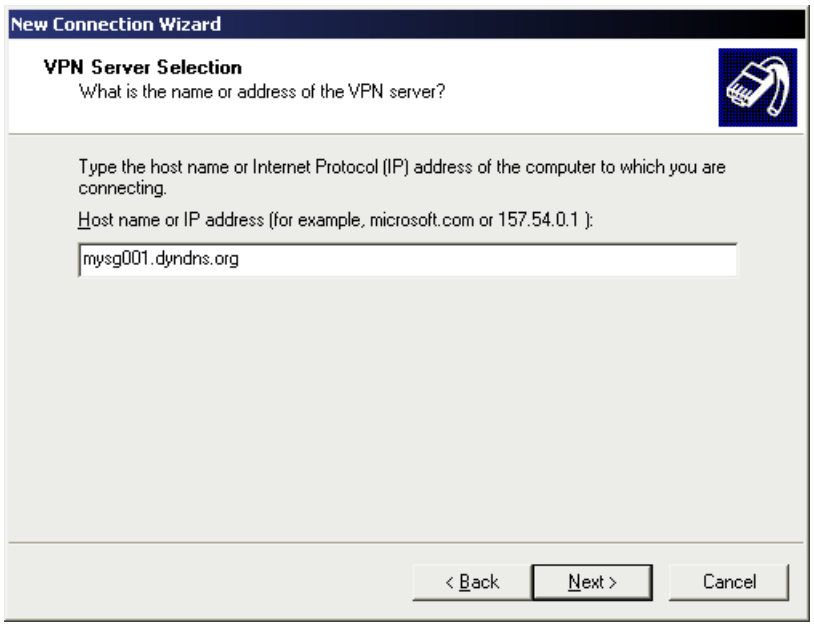

New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.
< Back
Next >
Cancel

Select **Connect to the network at my workplace** and click **Next**. Select **Virtual Private Network connection** and click **Next**.


New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
Office
For example, you could type the name of your workplace or the name of a server you will connect to.
< Back
Next >
Cancel

Choose a **Connection Name** for the VPN connection, such as your company name or simply *Office*. Click **Next**.

If you have set up your computer to connect to your ISP using dial up, select **Automatically dial this initial connection** and your dial up account from the pull down menu. If not, or you wish to manually establish your ISP connection before the VPN connection, select **Do not dial the initial connection**. Click **Next**.


New Connection Wizard
VPN Server Selection
What is the name or address of the VPN server?
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.
Host name or IP address (for example, microsoft.com or 157.54.0.1):
mysg001.dyndns.org
< Back
Next >
Cancel

Enter the SG PPTP appliance's Internet IP address or fully qualified domain name and click **Next**. Select whether you wish make this connect available to all users and whether you wish to add a shortcut to your desktop and click **Finish**.

Your VPN client is now set up and ready to connect.

Connect the remote VPN client

Verify that you are connected to the Internet, or have set up your VPN connection to automatically establish an initial Internet connection.

Select the connection for the SG unit VPN.

Enter a username and password added in the *Configuring user accounts for VPN server* section and click **Connect**.

L2TP VPN Server

To setup an L2TP/IPSec connection from a remote Windows XP client to your SG unit and local network:

- Enable and configure the L2TP VPN server.
- Configure IPSec tunnel settings.
- Set up VPN user accounts on the SG unit and enable the appropriate authentication security.
- Configure the VPN clients at the remote sites. The client does not require special software, the SG L2TP Server supports the standard L2TP and IPSec client software included with Windows XP.
- Connect the remote VPN client.

L2TP server setup

Select **L2TP VPN Server** from the **VPN** section of the main menu.

L2TP VPN Server Setup
L2TP VPN Server
L2TP IPSec Configuration
L2TP Server Setup
The L2TP VPN server allows remote users (who are connected to the Internet) to connect to your local area network (LAN). The server is compatible with both Windows and Linux L2TP clients.
To make use of RADIUS or TACACS+, configure them first and then select them using the Authentication Database drop down box.
Enable L2TP Server
IP addresses to give to remote hosts
10.23.0.80-90
IP Address to Assign VPN Server
LAN (Switch A)
Authentication Scheme
Encrypted Authentication (MS-CHAP v2)
Required Encryption Level
Strong Encryption (MPPE 128 Bit)
Authentication Database
Local
Submit

Check **Enable L2TP Server**.

Enter the **IP Addresses to give to remote hosts**, this must be a free IP address, or range of free IP addresses, from the network (typically the LAN) that the remote users are assigned while connected to the SG unit.

If you have configured several network connections, select the one that you want to connect remote users to from the **IP Address to Assign VPN Server** pull down menu. This is typically a LAN interface or alias.

Select the weakest **Authentication Scheme** to accept, access is denied to remote users attempting to connect using an authentication scheme weaker than this. They are described below, from strongest to weakest.

- **Encrypted Authentication (MS-CHAP v2):** The strongest type of authentication to use. This is the recommended option.
- **Encrypted Authentication (MS-CHAP):** This is not a recommended encryption type and should only be used for older dialin clients that do not support MS-CHAP v2.
- **Weakly Encrypted Authentication (CHAP):** This is the weakest type of encrypted password authentication to use. It is not recommended that clients connect using this as it provides very little password protection. Also note that clients connecting using CHAP are unable to encrypt traffic.

- **Unencrypted Authentication (PAP):** This is plain text password authentication. When using this type of authentication, the client passwords is transmitted un-encrypted.

Select the **Required Encryption Level**, access is denied to remote users attempting to connect not using this encryption level. Using **Strong Encryption (MPPE 128 Bit)** is recommended.

Select the **Authentication Database**. This allows you to indicate where the list of valid clients can be found. You can select from the following options:

- **Local:** Use the local database defined on the **Local Users** tab of the **Users** page. You must enable the **Dialin Access** option for the individual users that are allowed dialin access.
- **RADIUS:** Use an external RADIUS server as defined on the **RADIUS** tab of the **Users** page.
- **TACACS+:** Use an external TACACS+ server as defined on the **TACACS+** tab of the **Users** page.

Note

See the Users *section of the chapter entitled* System *for details on adding user accounts for PPTP access, and configuring the SG unit to enable authentication against a RADIUS or TACACS+ server.*

Click **Submit**.

Add an IPSec tunnel

Select **L2TP VPN Server** from the **VPN** section of the main menu and click the **L2TP IPSec Configuration** tab. Any existing L2TP IPSec tunnels are displayed, alongside icons to **Modify** and **Delete** them.

Authentication is performed using x.509 certificates or a pre-shared secret. You may add a single shared secret tunnel for *all* remote clients authenticating using shared secrets, an x.509 certificate tunnel for *each* remote client authenticating using certificates, or both.

- Select **Shared Secret Tunnel** to use a common secret (passphrase) that is shared between the SG unit and the remote client. This authentication method is relatively simple to configure, and relatively secure.

Note

Only one shared secret tunnel may be added. The one shared secret is used by all remote clients to authenticate.

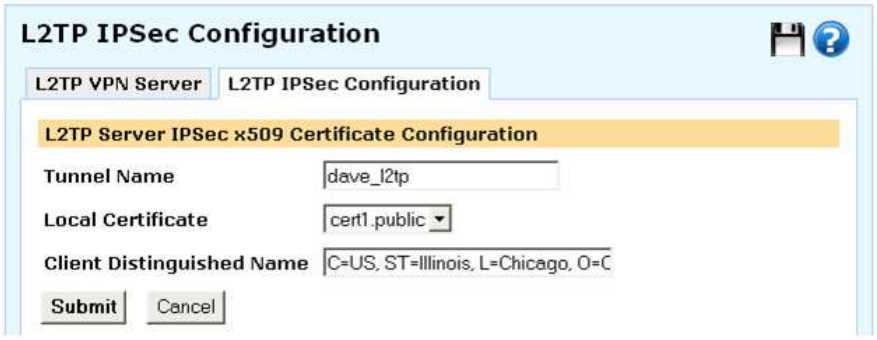
- Select **x.509 Certificate Tunnel** to use x.509 certificates to authenticate the remote client against a Certificate Authority's (CA) certificate. The CA certificate must have signed the local certificates that are used for tunnel authentication. Certificates need to be uploaded to the SG unit before a tunnel can be configured to use them (see *Certificate Management* in the *IPSec* section later in this chapter). This authentication method is more difficult to configure, but very secure.

  Creating and adding x.509 certificates is detailed in *Certificate Management* in the *IPSec* section later in this chapter.

Note

Multiple x.509 certificate tunnels may be added. A separate x.509 certificate tunnel is required for each remote client to authenticate.

Click **New**.



Enter a **Tunnel Name** to identify this connection. It may not be the same as any other L2TP/IPSec or regular IPSec tunnel names.

If adding a **Shared Secret Tunnel**, enter the **Shared Secret**. Ensure it is something hard to guess. Keep note of the shared secret, as it is used in configuring the remote client.

If adding an **x.509 Certificate Tunnel**, select the **Local Certificate** that you have uploaded to the SG unit. Enter the **Client Distinguished Name**; it must match exactly the distinguished name of the remote party's local certificate to successfully authenticate the tunnel. Distinguished name fields are listed

Note

Certificates need to be uploaded to the SG unit before a tunnel can be configured to use them (see Certificate Management *in the* IPSec *section later in this chapter).*

Add an L2TP user account

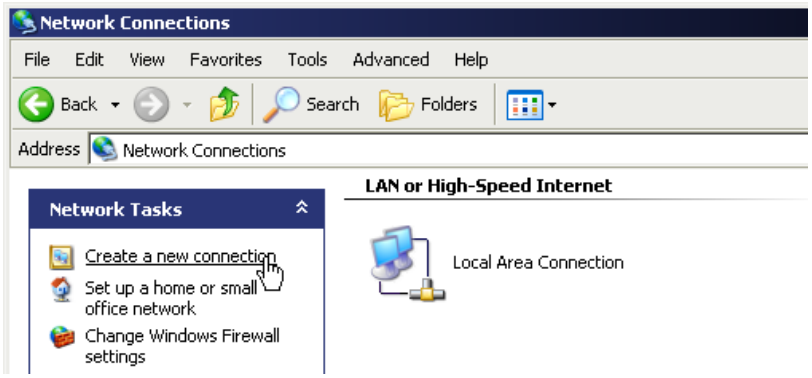
Select **Users** under **System** from the main menu, click **Local Users** and a **New** user with **PPTP Access**. Keep note of the **Username** and **Password**, as these are required in configuring the remote PPTP client.

Refer to the the *Users* section of the chapter entitled *System* for a more detailed account of adding a new local user.

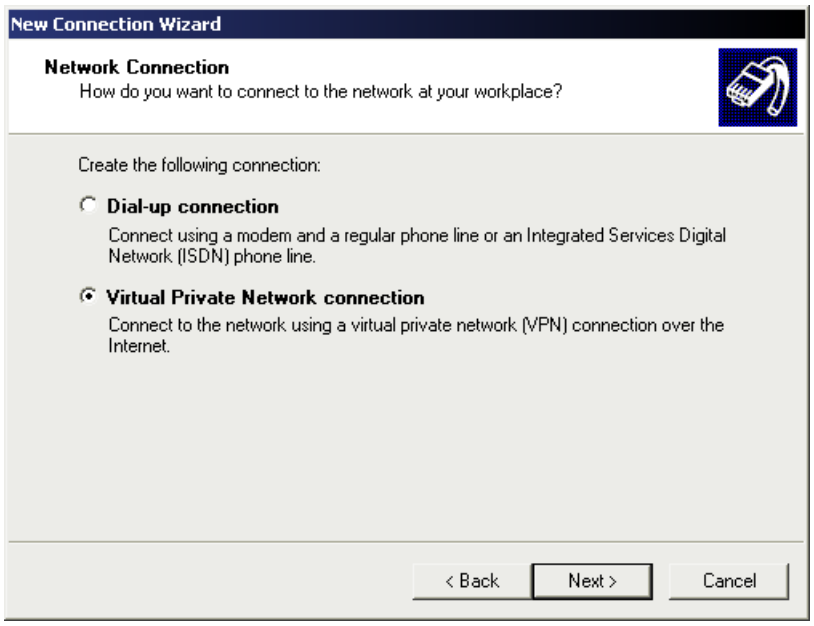
Configure the remote L2TP client

The following instructions are for Windows XP.

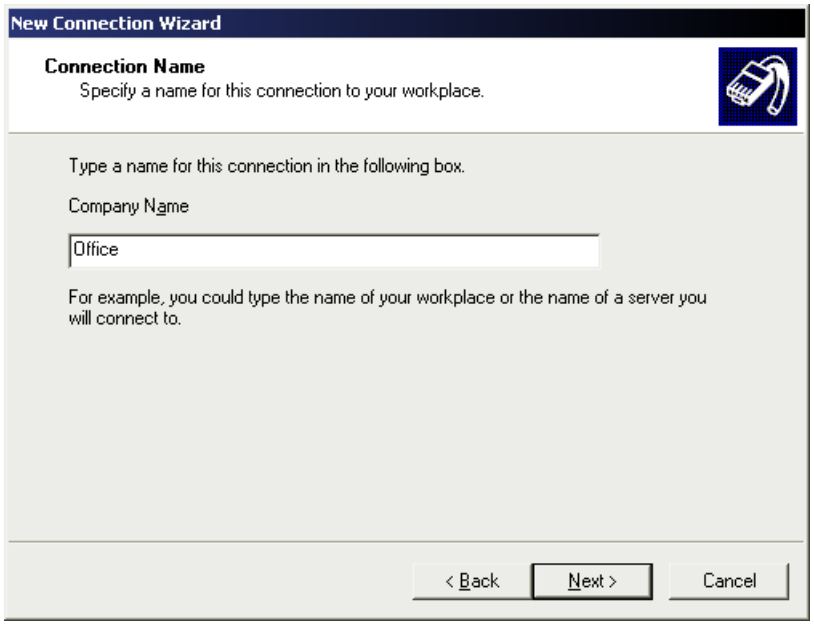
Log in as *Administrator* or with Administrator privileges. From the **Start** menu, select **Settings** and then **Network Connections**.



Click **Create New Connection** from the **Network Tasks** menu to the left.

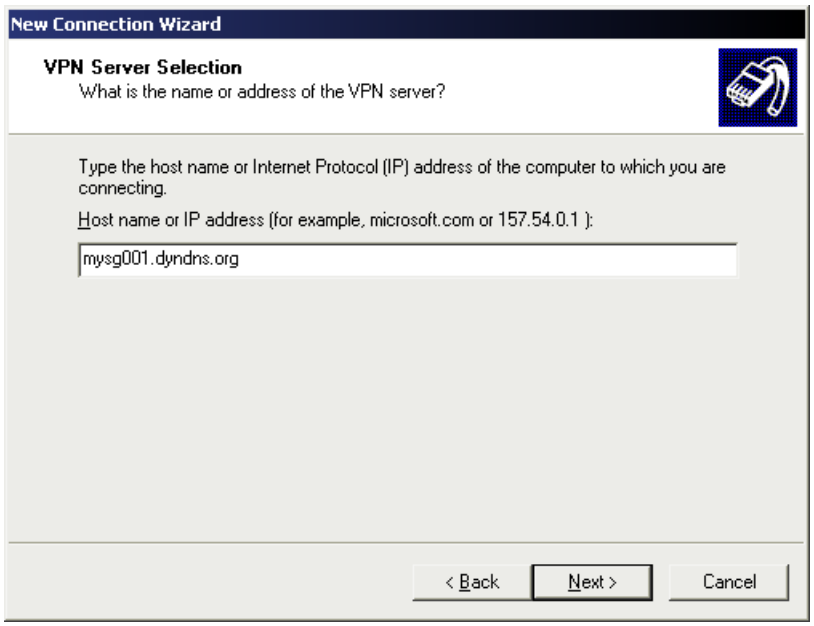

New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.
< Back
Next >
Cancel

Select **Connect to the network at my workplace** and click **Next**. Select **Virtual Private Network connection** and click **Next**.


New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
Office
For example, you could type the name of your workplace or the name of a server you will connect to.
< Back
Next >
Cancel

Choose a **Connection Name** for the VPN connection, such as your company name or simply *Office*. Click **Next**.

If you have set up your computer to connect to your ISP using dial up, select **Automatically dial this initial connection** and your dial up account from the pull down menu. If not, or you wish to manually establish your ISP connection before the VPN connection, select **Do not dial the initial connection**. Click **Next**.


New Connection Wizard
VPN Server Selection
What is the name or address of the VPN server?
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.
Host name or IP address (for example, microsoft.com or 157.54.0.1):
mysg001.dyndns.org
< Back
Next >
Cancel

Enter the SG PPTP appliance's Internet IP address or fully qualified domain name and click **Next**. Select whether you wish make this connect available to all users and whether you wish to add a shortcut to your desktop and click **Finish**.

- To authenticate using a **Shared Secret Tunnel**, click **Properties** on the **Connect *Connection Name*** dialog.

Click **Security -> IPSec Settings**, check **Use pre-shared key for authenticate** and in **Key** enter the **Shared Secret** you selected when configuring the shared secret tunnel on the SG unit.

- To authenticate using an **x.509 Certificate Tunnel**, you must first install the local certificate. The distinguished name of this local certificate must match that entered in **Client Distinguished Name** when configuring the x.509 certificate tunnel on the SG unit.

  See *Certificate Management* and *Using certificates with Windows IPSec* in the *IPSec* section later in this chapter for details on creating, packaging and adding certificates for use by Windows IPSec.

  Note

  Once a certificate added, Windows IPSec automatically uses it to attempt to authenticate the connection. If more than one certificate is installed, it tries each of them in turn.

  Authentication fails if the Windows client's certificate and the SG unit's certificate are not signed by the same certificate authority.

Your VPN client is now set up and ready to connect.

Connect the remote VPN client

Verify that you are connected to the Internet, or have set up your VPN connection to automatically establish an initial Internet connection.

Select the connection for the SG unit VPN.

Enter a username and password added in the *Configuring user accounts for VPN server* section and click **Connect**.

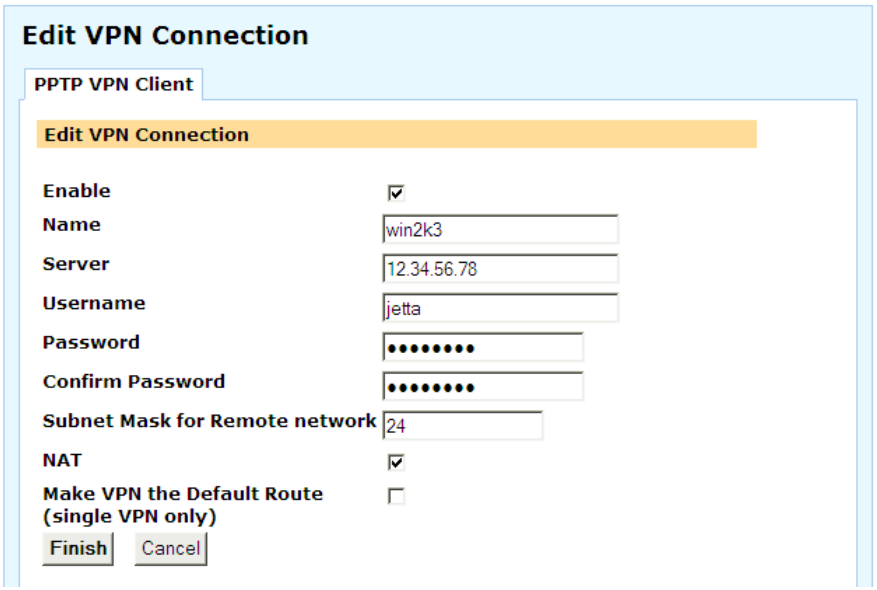
PPTP and L2TP VPN Client

The PPTP and L2TP client enables the SG unit to establish a VPN to a remote network running a PPTP or L2TP server (usually a Microsoft Windows server).

Although the VPN protocols are different, configuration of client tunnels is exactly the same.

Select **PPTP VPN Client** or **L2TP VPN Client** from the **VPN** section of the main menu. Any existing client tunnels are displayed alongside icons to **Enable/Disable**, **Delete**, and **Edit** them.

To add a new tunnel, click **New**.



Ensure **Enable** is checked, and enter:

- A descriptive **Name** for the VPN connection. This may describe the purpose for the connection.
- The remote PPTP or L2TP **Server** IP address to connect to.
- A **Username** and **Password** to use when logging in to the remote VPN. You may need to obtain this information from the system administrator of the remote PPTP server.
- Optionally, the **Subnet Mask for Remote network**. This is used to determine which packets should go the remote network.
- Check **NAT** to masquerade your local network behind the IP address on the remote network that the remote PPTP or L2TP server allocates the SG unit.
- Check **Make VPN the default route (single VPN only)** if you have a single VPN and want traffic from your local network to be routed through the tunnel instead of straight out onto the Internet.

Click **Finish**.

A PPTP status icon appears in the system tray on the bottom right hand side of your computer, informing you that you are connected.

You can now check your e-mail, use the office printer, access shared files and and computers on the network as if you were physically on the LAN.

Note

Depending on how your remote network is set up, some additional configuration may be required to enable browsing the network (aka ***Network Neighborhood*** *or* ***My Network Places****). Refer to the following knowledge base article for further details:*

http://www.cyberguard.com/snapgear/faqomatic/public_html/fom-serve/cache/70.html

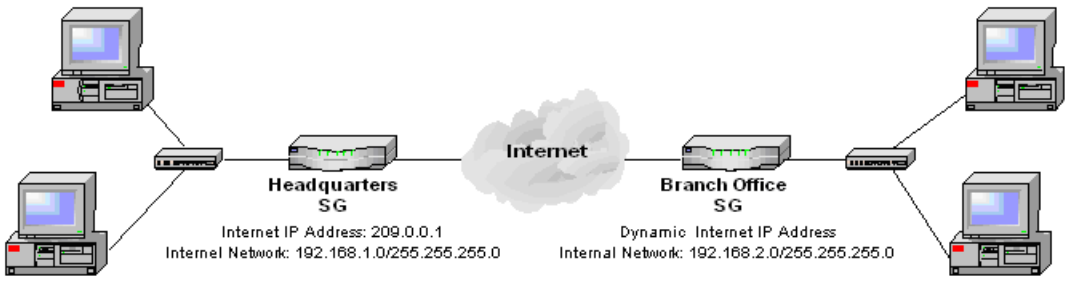
To disconnect, right click the PPTP Status system tray icon and select **Disconnect**.

You can then disconnect from the Internet if you wish.

IPSec

SG unit to SG unit

There are many possible configurations in creating an IPSec tunnel. The most common and simplest is described in this section. Additional options are also explained throughout this example, should it become necessary to configure the tunnel with those settings. For most applications to connect two offices together, a network similar to the following is used.

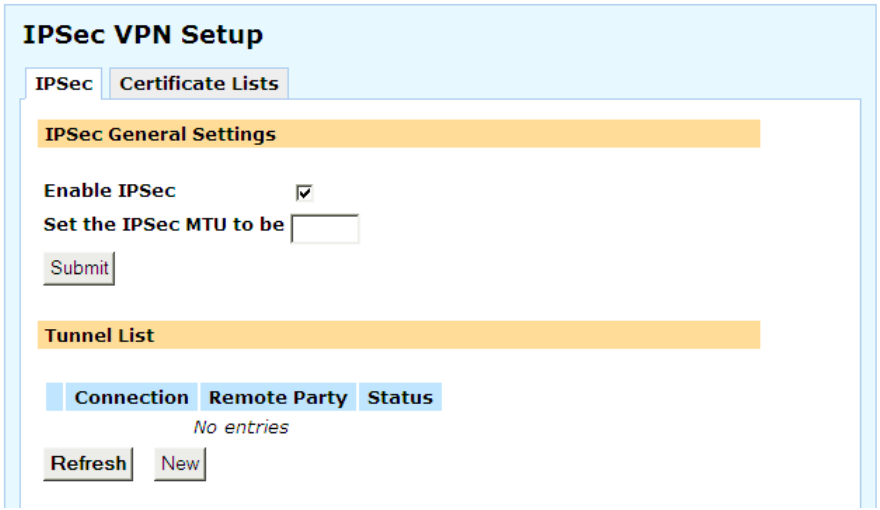


To combine the Headquarters and Branch Office networks together, an IPSec tunnel must be configured on both SG units.

Set Up the Branch Office

Enable IPSec

Select **IPSec** from the **VPN** section of the main menu. A page similar to the following is displayed.



Check the **Enable IPSec** checkbox.

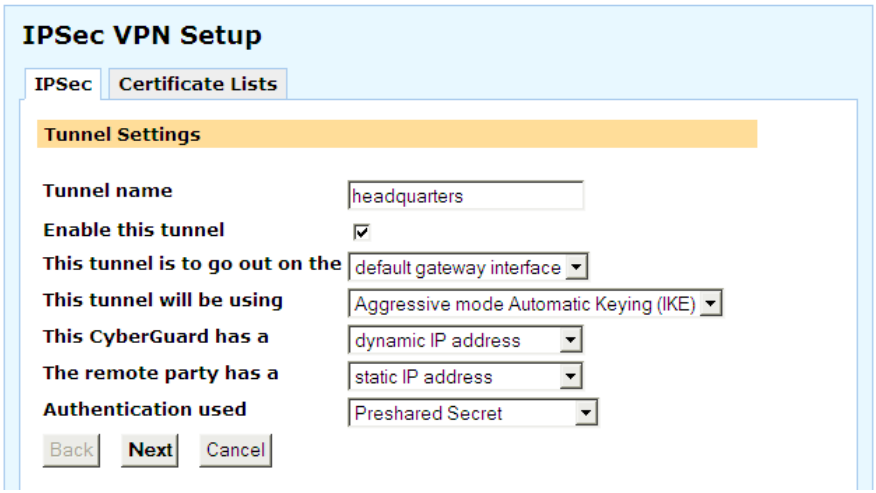
The Maximum Transmission Unit (**MTU**) of the IPSec interface can be configured filling in the desired MTU value in **IPSec MTU**. For most applications this need not be configured, however if it is set, the MTU value should be between 1400 and 1500. In this example leave the checkbox unchecked. Click the **Submit** button to save the changes.

Warning

It may be necessary to reduce the MTU of the IPSec interface if large packets of data are not being transmitted.

Configure a tunnel to connect to the headquarters office

To create an IPSec tunnel, click the **IPSec** link on the left side of the web management console and then click the **New** button under **Tunnel List**. A window similar to the following is displayed.



Tunnel settings page

Fill in the **Tunnel name** field with an apt description for the tunnel. The name must not contain spaces or start with a number. In this example, enter *Headquarters*.

Leave the **Enable this tunnel** checkbox checked.

Select the interface the IPSec tunnel is to go out on. The options depend on what is currently configured on the SG unit. For the vast majority of setups, this is the **default gateway interface** to the Internet. In this example, select the **default gateway interface** option.

Note

Select an interface other than the default gateway when you have more than one Internet connection or have configured aliased Internet interfaces, and require the IPSec tunnel to run on an interface other than the default gateway.

Select the type of keying for the tunnel to use. The SG unit supports the following types of keying:

- **Main Mode** automatically exchanges encryption and authentication keys and protects the identities of the parties attempting to establish the tunnel.

  This mode is the most secure, but difficult to configure in environments where one end has a dynamic Internet IP address.

- **Aggressive Mode** automatically exchanges encryption and authentication keys and uses less messages in the exchange when compared to main mode.

  Aggressive mode is typically used to allow parties that are configured with a dynamic IP address and a preshared secret to connect or if the SG unit or the remote party is behind a NAT device.

  This mode is less secure than main mode, but much easier to configure in environments where one end has a dynamic Internet IP address. When using this mode, ensure to use a long and particularly hard to guess preshared secret.

- **Manual Keying** requires the encryption and authentication keys to be specified. This mode is not recommended unless connecting to a legacy device that does not support main or aggressive modes.

  It is hard to identify problems Manual keying requires regular user intervention in the form of manual key changes, and it is hard to identify

In this example, select the **Aggressive Mode** option.

An IPSec tunnel connects two endpoints. These endpoints may be of different types, however some configurations are preferable to others with regards to ease of configuration and security (i.e. main vs. aggressive mode) and robustness (i.e. relying on an external DNS server). The following is a list of configurations, from most to least preferable:

1. **static IP address** to **static IP address**

2. **dynamic IP address** to **static IP address** (as detailed in this example)

3. **DNS hostname address** to **static IP address**

4. **DNS hostname address** to **DNS hostname address**

5. **DNS hostname address** to **dynamic IP address**

Select the type of IPSec endpoint this SG unit has on the interface on which the tunnel is going out. The SG unit can either have a **static IP**, **dynamic IP** or **DNS hostname address**. If a dynamic DNS service is to be used or there is a DNS hostname that resolves to the IP address of the port, then the DNS hostname address option should be selected. In this example, select **dynamic IP address**.

Select the type of IPSec endpoint the remote party has. The remote endpoint can have a **static IP address**, **dynamic IP address** or a **DNS hostname address**. In this example, select the **static IP address** option.

Select the type of authentication for the tunnel to use. The SG unit supports the following types of authentication:

- **Preshared Secret** is a common secret (passphrase) that is shared between the SG unit and the remote party.

  This authentication method is widely supported, relatively simple to configure, and relatively secure, although it is somewhat less secure when used with aggressive mode keying.

- **RSA Digital Signatures** uses a public/private RSA key pair for authentication. The SG unit can generate these key pairs. The public keys need to be exchanged between the SG unit and the remote party in order to configure the tunnel.

  This authentication method is not widely support, but is relatively secure and allows dynamic endpoints to be used with main mode keying.

- **x.509 Certificates** are used to authenticate the remote party against a Certificate Authority's (CA) certificate. The CA certificate must have signed the local certificates that are used for tunnel authentication. Certificates need to be uploaded to the SG unit before a tunnel can be configured to use them (see *Certificate Management*).

  This authentication method is widely supported and very secure, however differering terminology between vendors can make it difficult to set up a tunnel between a SG unit and an appliance from another vendor. This authentication method allows dynamic endpoints to be used with main mode keying.

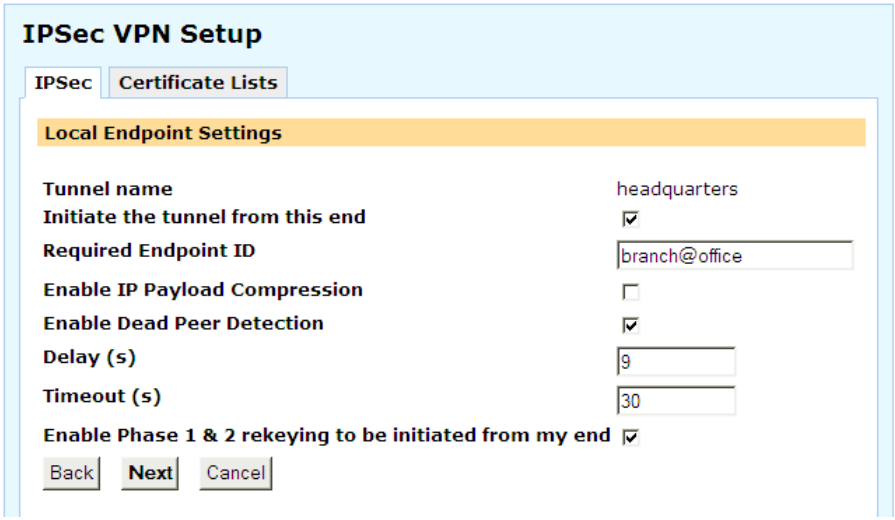
- **Manual Keys** establishes the tunnel using predetermined encryption and authentication keys.

  This authentication method is no longer widely used. It is not very secure as changing keys requires user intervention, and consequently keys are not changed very often. Using manual keys is not recommended.

In this example, select the **Preshared Secret** option.

Click the **Next** button to configure the **Local Endpoint Settings**.

Local endpoint settings



Leave the **Initiate the tunnel from this end** checkbox checked.

Note

This option is not be available when the SG unit has a static IP address and the remote party has a dynamic IP address.

Enter the **Required Endpoint ID** of the SG unit. This ID is used to authenticate the SG unit to the remote party. It is required because the SG unit in this example has a dynamic IP address. This field is also required if RSA Digital Signatures are used for authentication.

It becomes optional if the SG unit has a static IP address and is using Preshared Secrets for authentication. If it is optional and the field is left blank, the **Endpoint ID** defaults to the static IP address.

Note

If the remote party is a SG unit, the ID must have the form abcd@efgh*. If the remote party is not a SG unit, refer the interoperability documents on the SG Knowledge Base (http://www.cyberguard.com/snapgear/knowledgebase.html) to determine what form it must take. In this example, enter:* ***branch@office***

Leave the **Enable IP Payload Compression** checkbox unchecked. If compression is selected, *IPComp* compression is applied before encryption.

Check the **Enable Dead Peer Detection** checkbox. This allows the tunnel to be restarted if the remote party stops responding. This option is only used if the remote party supports Dead Peer Detection. It operates by sending notifications and waiting for acknowledgements.

Enter the **Delay** and **Timeout** values for Dead Peer Detection. The default times for the delay and timeout options are 9 and 30 seconds respectively. This means that a Dead Peer Detection notification is sent every 9 seconds (**Delay**) and if no response is received in 30 seconds (**Timeout**) then the SG unit attempts to restart the tunnel. In this example, leave the delay and timeout as their default values.

Leave the **Enable Phase 1 & 2 rekeying to be initiated from my end** checkbox checked. This enables automatic renegotiation of the tunnel when the keys are about to expire.

Click the **Next** button to configure the **Remote Endpoint Settings**.

Other options

The following options become available on this page depending on what has been configured previously:

- **Route to remote endpoint** is the next gateway IP address or *nexthop* along the previously selected IPSec interface. This field becomes available if an interface other than the default gateway was selected for the tunnel to go out on.

- **SPI Number** is the *Security Parameters Index*. It is a hexadecimal value and must be unique. It is used to establish and uniquely identify the tunnel. The SPI is used to determine which key is used to encrypt and decrypt the packets. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits and be in the range of *0x100-0xfff*. This field appears when **Manual Keying** has been selected.

- **Authentication Key** is the *ESP Authentication Key*. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 32 characters long when using MD5 or 40 characters long when using SHA1 (excluding any underscore characters). This field appears when **Manual Keying** has been selected.

- **Encryption Key** is the *ESP Encryption Key*. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 16 characters long when using DES or 48 characters long when using 3DES (excluding any underscore characters). This field appears when **Manual Keying** has been selected.

- **Cipher and Hash** pull down menu contains the ESP encryption/authentication algorithms that can be used for the tunnel. The option selected must correspond to the encryption and authentication keys used. This pull down menu appears when **Manual Keying** has been selected. The options include the following:

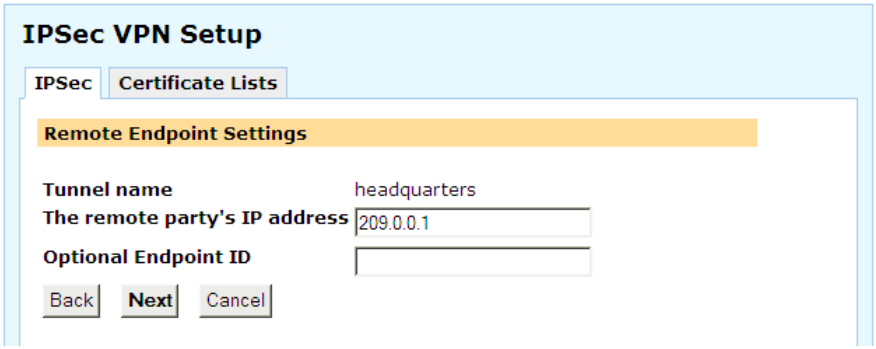
    - **3des-md5-96** uses the encryption transform following the Triple-DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and MD5 (96-bit authenticator). It uses a 192-bit 3DES encryption key and a 128-bit HMAC-MD5 authentication key.

    - **3des-sha1-96** uses the encryption transform following the Triple-DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and SHA1 (96-bit authenticator). It uses a 192-bit 3DES encryption key and a 160-bit HMAC-SHA1 authentication key.

    - **des-md5-96** uses the encryption transform following the DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and MD5 (96-bit authenticator). It uses a 56-bit 3DES encryption key and a 128-bit HMAC-MD5 authentication key.

    - **des-sha1-96** uses the encryption transform following the DES standard in Cipher-Block-Chaining mode with authentication provided by HMAC and SHA1 (96-bit authenticator). It uses a 56-bit DES encryption key and a 160-bit HMAC-SHA1 authentication key.

- **Local Network** is the network behind the local SG unit. This field appears when **Manual Keying** has been selected.



Enter the Internet IP address of the remote party in **The remote party's IP address** field. In this example, enter: **209.0.0.1**

The **Endpoint ID** is used to authenticate the remote party to the SG unit. The remote party's ID is optional if it has a static IP address and uses Preshared Secrets for authentication. It becomes a required field if the remote party has a dynamic IP or DNS hostname address or if RSA Digital Key Signatures are used for authentication. It is optional in this example, because the remote party has a static IP address. If the remote party is a SG unit, it must have the form *abcd@efgh*. If the remote party is not a SG unit, refer the interoperability documents on the SG Knowledge Base (http://www.cyberguard.com/snapgear/knowledgebase.html) to determine what form it must take. In this example leave the field blank.

Click the **Next** button to configure the **Phase 1 Settings**.

Other options

The following options become available on this page depending on what has been configured previously:

- **The remote party's DNS hostname address** field is the DNS hostname address of the Internet interface of the remote party. This option becomes available if the remote party has been configured to have a DNS hostname address.
- **Distinguished Name** field is the list of attribute/value pairs contained in the certificate. The list of attributes supported are as follows:

C	Country
ST	State or province
L	Locality or town
O	Organization

OU	Organizational Unit
CN	Common Name
N	Name
G	Given name
S	Surname
I	Initials
T	Personal title
E	E-mail
Email	E-mail
SN	Serial number
D	Description
TCGID	[Siemens] Trust Center Global ID

The attribute/value pairs must be of the form *attribute=value* and be separated by commas. For example : C=US, ST=Illinois, L=Chicago, O=SecureComputing, OU=Sales, CN=SG550. It must match exactly the **Distinguished Name** of the remote party's local certificate to successfully authenticate the tunnel. This field appears when **x.509 Certificates** has been selected.

- **RSA Key Length** pull down menu allows the length of the SG unit generated RSA public/private key pair to be specified. The options include 512, 1024, 1536 and 2048 bits. The greater the key pair length, the longer the time required to generate the keys. It may take up to 20 minutes for a 2048 bit RSA key to be generated. This option appears when RSA Digital Key Signatures has been selected.

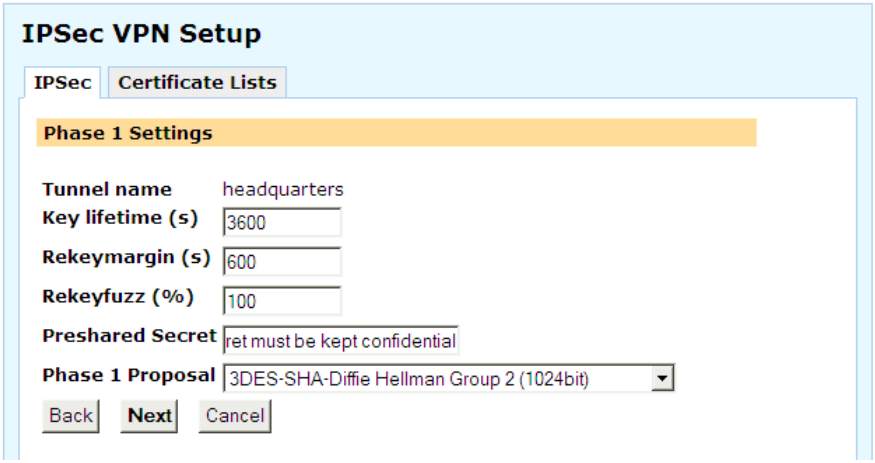
- **SPI Number** field is the *Security Parameters Index*. However, this applies to the remote party. It is a hexadecimal value and must be unique. It is used to establish and uniquely identify the tunnel. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits and be in the range of *0x100-0xfff*. This field appears when **Manual Keying** has been selected.

- **Authentication Key** field is the ESP Authentication Key. However, this applies to the remote party. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 32 characters long when using MD5 or 40 characters long when using SHA1 (excluding any underscore characters). It must use the same hash as the SG unit's authentication key. This field appears when **Manual Keying** has been selected.

- **Encryption Key** field is the ESP Encryption Key. However, this applies to the remote party. It must be of the form 0x*hex*, where *hex* is one or more hexadecimal digits. The *hex* part must be exactly 16 characters long when using DES or 48 characters long when using 3DES (excluding any underscore characters). It must use the same cipher as the SG unit's encryption key. This field appears when **Manual Keying** has been selected.

- **Remote Network** is the network behind the remote party. This field appears when **Manual Keying** has been selected.

Phase 1 settings



Set the length of time before Phase 1 is renegotiated in the **Key lifetime (s)** field. The length may vary between 60 and 86400 minutes. Shorter values offer higher security at the expense of the computational overhead required to calculate new keys. For most applications 3600 seconds is recommended. In this example, leave the **Key Lifetime** as the default value of 3600 seconds.

A new Phase 1 key can be renegotiated before the current one expires. The time for when this new key is negotiated before the current key expires can be set in the **Rekeymargin (s)** field. In this example, leave the **Rekeymargin** as the default value of 600 seconds.

The **Rekeyfuzz** value refers to the maximum percentage by which the **Rekeymargin** should be randomly increased to randomize rekeying intervals. The **Key lifetimes** for both Phase 1 and Phase 2 are dependent on these values and must be greater that the value of "**Rekeymargin x (100 + Rekeyfuzz) / 100**." In this example, leave the **Rekeyfuzz** as the default value of 100%.

Enter a secret in the **Preshared Secret** field. Keep a record of this secret as it is used to configure the remote party's secret. In this example, enter: **This secret must be kept confidential**

Warning

The secret must be entered identically at each end of the tunnel. The tunnel fails to connect if the secret is not identical at both ends. The secret is a highly sensitive piece of information. It is essential to keep this information confidential. Communications over the IPSec tunnel may be compromised if this information is divulged.

Select a **Phase 1 Proposal**. Any combination of the ciphers, hashes and Diffie Hellman groups that the SG unit supports can be selected. The supported ciphers are *DES* (56 bits), *3DES* (168 bits) and *AES* (128, 196 and 256 bits). The supported hashes are *MD5* and *SHA* and the supported Diffie Hellman groups are *1* (768 bit), *2* (1024 bit) and *5* (1536 bits). The SG unit also supports extensions to the Diffie Hellman groups to include 2048, 3072 and 4096 bit Oakley groups. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option. Click the **Next** button to configure the **Phase 2 Settings**.

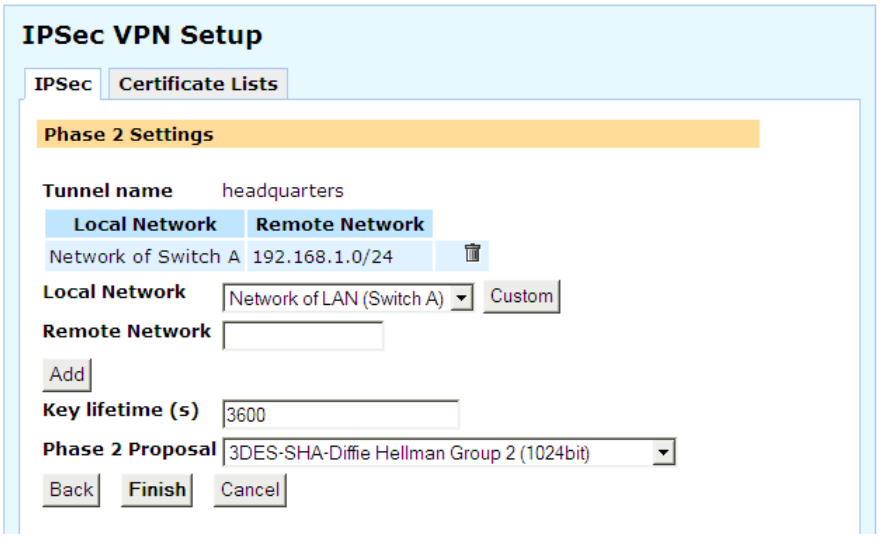
Other options

The following options become available on this page depending on what has been configured previously:

- **Local Public Key** field is the public part of the RSA key generated for RSA Digital Signatures authentication. These fields are automatically populated and do not need to be modified unless a different RSA key is to be used. This key must be entered in the Remote Public Key field of the remote party's tunnel configuration. This field appears when **RSA Digital Signatures** has been selected.
- **Remote Public Key** field is the public part of the remote party's RSA Key generated for RSA Digital Key authentication. This field must be populated with the remote party's public RSA key. This field appears when **RSA Digital Signatures** has been selected.

- **Local Certificate** pull down menu contains a list of the local certificates that have been uploaded for x.509 authentication. Select the required certificate to be used to negotiate the tunnel. This field appears when **x.509 Certificates** has been selected.

Phase 2 settings page



Specify the **Local Network**s and **Remote Network**s to link together with the IPSec tunnel. For the **Local Network**, you may use a **Predefined** network, or enter a **Custom** network address. You must **Add** at least one local and one remote network.

Note

*Only network traffic that is coming from a **Local Network** and is destined for a **Remote Network** is allowed across the tunnel. IPSec uses its own routing mechanisms, and disregards the main routing table.*

For this example, select **Network of LAN** for the **Local Network**, and enter **192.168.1.0/24** for the **Remote Network** and click **Add**.

Set the length of time before Phase 2 is renegotiated in the **Key lifetime (s)** field. The length may vary between 1 and 86400 seconds. For most applications 3600 seconds is recommended. In this example, leave the **Key Lifetime** as the default value of 3600 seconds.

Select a **Phase 2 Proposal**. Any combination of the ciphers, hashes and Diffie Hellman groups that the SG unit supports can be selected. The supported ciphers are *DES*, *3DES* and *AES* (128, 196 and 256 bits). The supported hashes are *MD5* and *SHA* and the supported Diffie Hellman group are *1* (768 bit), *2* (1024 bit) and *5* (1536 bits). The SG unit also supports extensions to the Diffie Hellman groups to include 2048, 3072 and 4096 bit Oakley groups. *Perfect Forward Secrecy* is enabled if a Diffie-Hellman group or an extension is chosen. Phase 2 can also have the option to not select a Diffie Hellman Group, in this case *Perfect Forward Secrecy* is not enabled. *Perfect Forward Secrecy* of keys provides greater security and is the recommended setting. In this example, select the **3DES-SHA-Diffie Hellman Group 2** (1024 bit) option.

Click the **Finish** button to save the tunnel configuration.

Configuring the Headquarters

Enable IPSec

Click the **IPSec** link on the left side of the web management console.

Check the **Enable IPSec** checkbox.

Select the type of IPSec endpoint the SG unit has on its Internet interface. In this example, select **static IP address**.

Leave the **IPSec MTU** unchanged.

Click the **Apply** button to save the changes.

Configure a tunnel to accept connections from the branch office

To create an IPSec tunnel, click the **IPSec** link on the left side of the web management console, then click **New**. Many of the settings such as the **Preshared Secret**, **Phase 1** and **2 Proposal**s and **Key Lifetime**s are the same as the branch office.

Tunnel settings page

Fill in the **Tunnel name** field with an apt description of the tunnel. The name must not contain spaces or start with a number. In this example, enter: *Branch_Office*

Leave checked the **Enable this tunnel** checkbox.

Select the Internet interface the IPSec tunnel is to go out on. In this example, select **default gateway interface** option.

Select the type of keying for the tunnel to use. In this example, select the **Aggressive mode with Automatic Keying (IKE)** option.

Select the type of IPSec endpoint this SG unit has. In this example, select the **static IP address** option.

Select the type of IPSec endpoint the remote party has. In this example, select the **dynamic IP address** option.

Select the type of authentication for the tunnel to use. In this example, select the **Preshared Secret** option.

Click the **Next** button to configure the **Local Endpoint Settings**.

Local endpoint settings page

Leave the **Optional Endpoint ID** field blank in this example. It is optional because this SG unit has a static IP address. If the remote party is a SG unit and an Endpoint ID is used, it must have the form *abcd@efgh*. If the remote party is not a SG unit refer the interoperability documents on the SG Knowledge Base to determine what form it must take (http://www.cyberguard.com/snapgear/knowledgebase.html).

Leave the **Enable IP Payload Compression** checkbox unchecked.

Leave the **Enable Phase 1 & 2 rekeying to be initiated from my end** checkbox checked.

Click the **Next** button to configure the **Remote Endpoint Settings**.

Remote endpoint settings page

Enter the **Required Endpoint ID** of the remote party. In this example, enter the **Local Endpoint ID** at the Branch Office which was: **branch@office**

Click the **Next** button to configure the **Phase 1 Settings**.

Phase 1 settings page

Set the length of time before Phase 1 is renegotiated in the **Key lifetime (s)** field. In this example, leave the **Key Lifetime** as the default value of 3600 minutes.

Set the time for when the new key is negotiated before the current key expires in the **Rekeymargin** field. In this example, leave the **Rekeymargin** as the default value of 600 seconds.

Set the maximum percentage by which the **Rekeymargin** should be randomly increased to randomize rekeying intervals in the **Rekeyfuzz** field. The **Key lifetimes** for both Phase 1 and Phase 2 are dependent on these values and must be greater that the value of "**Rekeymargin x (100 + Rekeyfuzz) / 100**." In this example, leave the **Rekeyfuzz** as the default value of 100%.

Enter a secret in the **Preshared Secret** field. This must remain confidential. In this example, enter the Preshared Secret used at the branch office SG unit, which was: **This secret must be kept confidential**

Select a **Phase 1 Proposal**. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option (same as the Branch Office **Phase 1 Proposal**).

Click the **Next** button to configure the **Phase 2 Settings**.

Phase 2 settings page

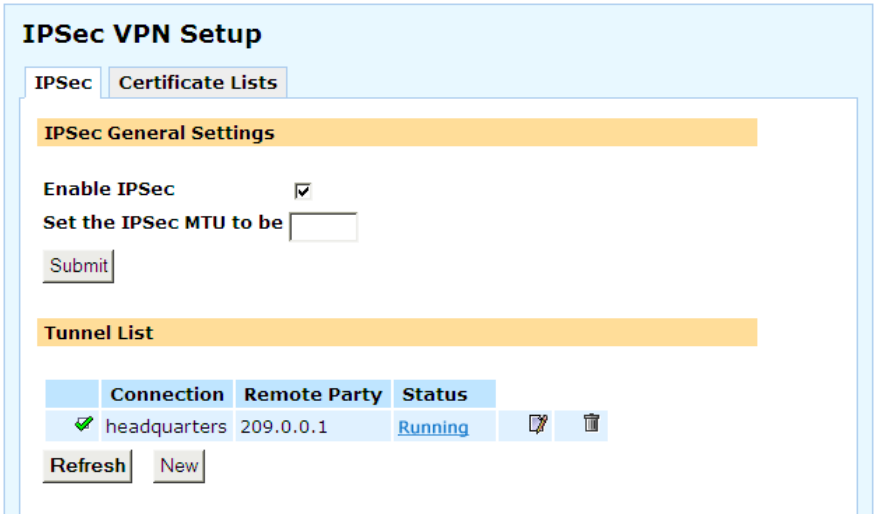
Select **Network of LAN (Switch A)** for the **Local Network**, enter **192.168.2.0/24** for the **Remote Network** and click **Add**.

Set the length of time before Phase 2 is renegotiated in the **Key lifetime (s)** field. In this example, leave the **Key Lifetime** as the default value of 600 seconds.

Select a **Phase 2 Proposal**. In this example, select the **3DES-SHA-Diffie Hellman Group 2 (1024 bit)** option (same as the Branch Ofiice **Phase 2 Proposal**).

Click the **Apply** button to save the tunnel configuration.

Tunnel List



Connection

Once a tunnel has been configured, an entry with the tunnel name in the **Connection** field is shown.

Note

*You may modify, delete or disable/enable a tunnel by clicking on the corresponding **Edit**, **Delete** or **Enable/Disable** icon.*

Remote party

The **Remote Party** which the tunnel is configured to connect to is defined either by its Endpoint ID, IP Address or Distinguished Name.

Click **Remote Party** to sort the tunnel list by the remote party ID/name/address.

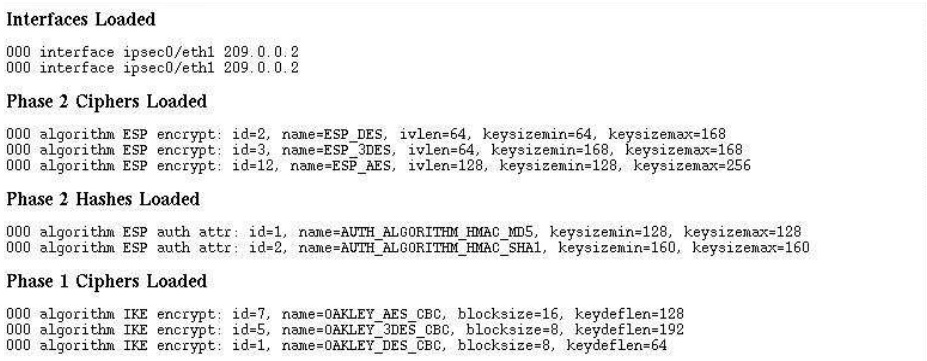
Status

Tunnels that use *Automatic Keying (IKE)* display one of four states in the **Status** field. The states include the following:

- **Down** indicates that the tunnel is not being negotiated. This may be due to the following reasons:
    - IPSec is disabled.
    - The tunnel is disabled.
    - The tunnel could not be loaded due to misconfiguration.
- **Negotiating Phase 1** indicates that IPSec is negotiating Phase 1 to establish the tunnel. Aggressive or Main mode packets (depending on tunnel configuration) are transmitted during this stage of the negotiation process.
- **Negotiating Phase 2** indicates that IPSec is negotiating Phase 2 to establish the tunnel. Quick mode packets are transmitted during this stage of the negotiation process.
- **Running** indicates that the tunnel has been established.

Tunnels that use *Manual Keying* are in either a **Down** or **Running** state.

For tunnels that use *Automatic Keying*, further negotiation details can be seen by clicking on the status. A window similar to the following is displayed.


Interfaces Loaded
000 interface ipsec0/eth1 209.0.0.2
000 interface ipsec0/eth1 209.0.0.2
Phase 2 Ciphers Loaded
000 algorithm ESP encrypt: id=2, name=ESP_DES, ivlen=64, keysizemin=64, keysizemax=168
000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=64, keysizemin=168, keysizemax=168
000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=128, keysizemin=128, keysizemax=256
Phase 2 Hashes Loaded
000 algorithm ESP auth attr: id=1, name=AUTH_ALGORITHM_HMAC_MD5, keysizemin=128, keysizemax=128
000 algorithm ESP auth attr: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, keysizemin=160, keysizemax=160
Phase 1 Ciphers Loaded
000 algorithm IKE encrypt: id=7, name=OAKLEY_AES_CBC, blocksize=16, keydeflen=128
000 algorithm IKE encrypt: id=5, name=OAKLEY_3DES_CBC, blocksize=8, keydeflen=192
000 algorithm IKE encrypt: id=1, name=OAKLEY_DES_CBC, blocksize=8, keydeflen=64

Interfaces Loaded lists the SG unit's interfaces which IPSec is using.

Phase 2 Ciphers Loaded lists the encryption ciphers that tunnels can be configured with for Phase 2 negotiations. This includes DES, 3DES and AES.

Phase 2 Hashes Loaded lists the authentication hashes that tunnels can be configured with for Phase 2 negotiations. This includes MD5 and SHA1 (otherwise known as SHA).

Phase 1 Ciphers Loaded lists the encryption ciphers that tunnels can be configured with for Phase 1 negotiations. This includes DES, 3DES and AES.

Phase 1 Hashes Loaded lists the authentication hashes that tunnels can be configured with for Phase 1 negotiations. This includes MD5 and SHA.

Diffie Hellman Groups Loaded lists the Diffie Hellman groups and Oakley group extensions that can be configured for both Phase 1 and Phase 2 negotiations.

Connection Details lists an overview of the tunnel's configuration. It contains the following information:

- An outline of the tunnel's network setup. In this example, it is *192.168.2.0/24===209.0.0.2(branch@office)...209.0.0.1===192.168.1.0/24*
- Phase 1 and Phase 2 key lifetimes (**ike_life** and **ipsec_life** respectively). In this example, they are both *3600s*.
- Type of automatic (IKE) keying. In this example, the **policy** line displays *AGGRESSIVE*. For Main mode, it displays *MAIN*.
- Type of authentication used. In this example, the **policy** line displays *PSK* (Preshared Key). For RSA Digital Signatures or x.509 certificates, it displays *RSA*.
- Whether Perfect Forward Secrecy is used. In this example, the **policy** line has the *PFS* keyword. If PFS is disabled, the keyword does not appear.
- Whether IP Payload Compression is used. In this example, the **policy** line does not have the *COMPRESS* keyword since it has not been enabled.
- The interface on which the tunnel is going out. In this example, the **interface** line has *eth1*, which is the Internet interface.
- The current Phase 1 key. This is the number that corresponds to the **newest ISAKMP SA** field. In this example, phase 1 has not be successfully negotiated, so there is no key yet.
- The current Phase 2 key. This is the number that corresponds to the **newest IPSec SA** field. In this example, phase 1 has not be successfully negotiated, so there is no key yet.
- The Phase 1 proposal wanted. The line **IKE algorithms wanted** reads *5_000-2-2*. The *5_000* refers to cipher 3DES (where 3DES has an id of 5, see Phase 1 Ciphers Loaded), the first *2* refer to hash SHA (where SHA has an id of 2, see Phase 1 Hashes Loaded) and the second *2* refer to the Diffie Hellman Group 2 (where Diffie Hellman Group 2 has an id of 2).

- The Phase 2 proposal wanted. The line **ESP algorithms wanted** reads *3_000-2; pfsgroup=2*. The *3_000* refers to cipher 3DES (where 3DES has an id of 3, see Phase 2 Ciphers Loaded), the *2* refers to hash SHA1 or SHA (where SHA1 has an id of 2, see Phase 2 Hashes Loaded) and *pfsgroup=2* refers to the Diffie Hellman Group 2 for Perfect Forward Secrecy (where Diffie Hellman Group 2 has an id of 2).

Negotiation State reports what stage of the negotiation process the tunnel is in. In this example it has *initiated* and sent the first aggressive mode packet (*AI1*) and is expecting its *response* (*AR1*) in the line *STATE_AGGR_I1 (sent AI1, expecting AR1)*. Once the Phase 1 has been successfully negotiated, the status displays *ISAKMP SA established*. Once the Phase 2 has been successfully negotiated, the status displays *IPSec SA established*. The tunnel is then established and running.

NAT Traversal Support

NAT Traversal allows tunnels to be established when the IPSec endpoints reside behind NAT devices. If any NAT devices are detected, the NAT Traversal feature is automatically used. It cannot be configured manually on the SG unit.

Dynamic DNS Support

Internet Service Providers generally charge higher fees for static IP addresses than for dynamic IP addresses when connecting to the Internet. The SG unit can reduce costs since it allows tunnels to be established with both IPSec endpoints having dynamic IP addresses. The two endpoints must, however, be SG units and at least one end must have *dynamic DNS* enabled. The SG unit supports a number of dynamic DNS providers. When configuring the tunnel, select the **DNS hostname address** type for the IPSec endpoint that has dynamic DNS supported and enable **Dead Peer Detection**. If the IP address of the SG unit's DNS hostname changes, the tunnel automatically renegotiates and establishes the tunnel.

Certificate Management

x.509 certificates can be used to authenticate IPSec endpoints during tunnel negotiation for Automatic Keying. The other methods are *Preshared Secrets* and *RSA Digital Signatures*.

Certificates need to be uploaded to the SG unit before they can be used in a tunnel. Certificates have time durations in which they are valid. Ensure that the certificates uploaded are valid and that the **Date and Time** settings have been set correctly on the SG unit.

The SG unit only supports certificates in *base64 PEM* or *binary DER* format.

Some certificate authorities (CA) distribute certificates in a *PKCS12* format file. This format combines the CA certificate, local public certificate and local private key certificate into one file. These certificates must be extracted before uploading them to the SG unit; see *Extracting certificates* further on.

If you do not have access to certificates issued by a certificate authority (CA), you may create self-signed certificates; see *Creating certificates* further on.

The OpenSSL application

The remainder of this section requires OpenSSL application, run from a Windows command prompt (**Start** -> **Run** -> type **cmd**) or Linux shell prompt.

A Windows version of OpenSSL is provided in the *openssl* directory of the SG CD. Ensure that this directory is in your execution path, or copy all files from this directory into a working directory on your hard drive.

For other operating systems, OpenSSL is available for free download at: http://www.openssl.org/

Extracting certificates

To extract the CA certificate, run:

```
openssl pkcs12 -nomacver -cacerts -nokeys -in pkcs12_file -out
ca_certificate.pem
```

.. where **pksc12_file** is the PKCS12 file issued by the CA and **ca_certificate.pem** is the CA certificate to be uploaded into the SG unit.

When the application prompts you to **Enter Import Password**, enter the password used to create the certificate. If none was used simply press enter.

To extract the local public key certificate type, enter the following at the Windows command prompt:

```
openssl pkcs12 -nomacver -clcerts -nokeys -in pkcs12_file -out
local_certificate.pem
```

.. where **pksc12_file** is the PKCS12 file issued by the CA and **local_certificate.pem** is the local public key certificate to be uploaded into the SG unit.

When the application prompts you to **Enter Import Password**, enter the password used to create the certificate. If none was used simply press enter.

To extract the local private key certificate type, enter the following at the Windows command prompt:

```
openssl pkcs12 -nomacver -nocerts -in pkcs12_file -out
local_private_key.pem
```

.. where **pksc12_file** is the PKCS12 file issued by the CA and **local_private_key.pem** is the local private key certificate to be uploaded into the SG unit.

When the application prompts you to **Enter Import Password**, enter the password used to create the certificate. If none was used simply press enter. When the application prompts you to **Enter PEM pass phrase**, choose a secure pass phrase that is greater than 4 characters long. This is the pass phrase used to secure the private key file, and is the same pass phrase you enter when uploading the private key certificate into the SG unit. Verify the pass phrase by typing it in again.

The SG unit also supports *Certificate Revocation List* (CRL) files. A CRL is a list of certificates that have been revoked by the CA before they have expired. This may be necessary if the private key certificate has been compromised or if the holder of the certificate is to be denied the ability to establish a tunnel to the SG unit.

Creating certificates

There are two steps to create self-signed certificates. First, create a single CA certificate, second, create one or more local certificate pairs and sign them with the CA certificate.

Create a CA certificate

Create the CA directory:

```
mkdir rootCA
```

Create the serial number for the first certificate:

```
echo 01 > rootCA/serial
```

Create an empty CA database file under Windows:

```
type nul > rootCA/index.txt
```

.. or under Linux:

```
touch rootCA/index.txt
```

Create the CA certificate, omit the **–nodes** option if you want to use a password to secure the CA key:

```
openssl req -config openssl.cnf -new -x509 -keyout
rootCA/ca.key -out rootCA/ca.pem -days DAYS_VALID -nodes
```

.. where *DAYS_VALID* is the number of days the root CA is valid for.

Create local certificate pairs

For each local certificate you wish to create, there are two steps.

First, create the certificate request:

```
openssl req -config openssl.cnf -new -keyout cert1.key -out
cert1.req
```

Enter a PEM pass phrase (this is the same pass phrase required when you upload the key to the SG unit) and then the certificate details. All but the **Common Name** are optional and may be omitted.

Second, sign the certificate request with the CA:

```
openssl ca -config openssl.cnf -out cert1.pem -notext -infiles
cert1.req
```

You now have a local certificate pair, the local public certificate *cert1.pem* and the local private key certificate *cert1.key*, ready to use in the SG unit.

For each certificate required, change the *cert1.** filenames appropriately.

Using certificates with Windows IPSec

To create certificates to use with IPSec on a Windows system, first follow the previous instructions in *Creating a CA certificate* and *Creating local certificate pairs*.

Windows IPSec requires the certificates to be in a PKCS12 format file. This format combines the CA certificate, local public certificate and local private key certificate into one file.

```
openssl pkcs12 -export -inkey cert1.key -in cert1.pem -certfile
rootCA/ca.pem -out cert1.p12 -name "Certificate 1"
```

To install the new PCKS12 file, *cert1.p12*, on Windows XP, open up the *Microsoft Management Console* (**Start** -> **Run** -> then type **mmc**).

Add the *Certificate Snap-in* (**File** -> **Add/Remove Snap-in** -> **Add** -> select **Certificates** -> **Add** -> select the account level you want the certificates installed for (i.e. current user vs. all users) (-> **Local Computer**) -> **Close** -> **OK**.

Double click **Certificates** to open the store.

Select the **Personal** store.

Import new certificate (**Action** -> **All Tasks** -> **Import**).

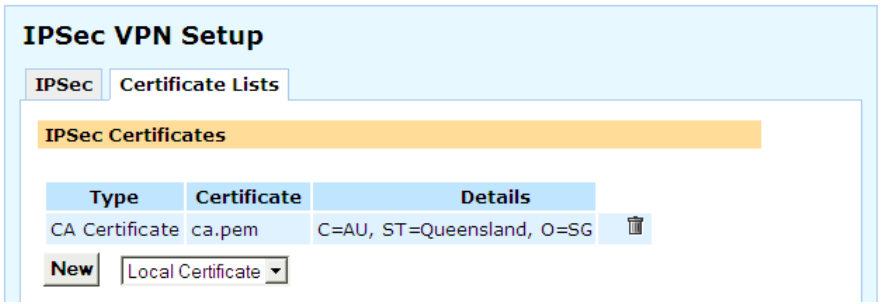
Locate *cert1.p12.*

Type in the **Export Password** if you used one.

Select **Automatically select the certificate store based on the type of certificate**.

Add certificates

To add certificates to the SG unit, select **IPSec** from the **VPN** section of the main menu and then click the **Certificate Lists** tab at the top of the window. Any previously uploaded certificates are displayed, and may be removed by clicking the corresponding **Delete** icon.



Select the certificate type click **New**. You may add a **CA Certificate** (Certificate Authority), **CRL Certificate** (Certificate Revocation List) or **Local Certificate**.

Click **Browse** to locate the certificate file or files.

If you are adding a **Local Certificate**, enter the *Public Key certificate* in **Local Certificate** the *Local Private Key certificate* in **Private Key Certificate**, and the passphrase to unlock the private key certificate in **Private Key Certificate Passphrase**. The certificate must be in *PEM* or *DER* format.

Certificates have time durations in which they are valid. Ensure that the certificates uploaded are valid and that the **Date and Time** settings have been set correctly on the SG unit.

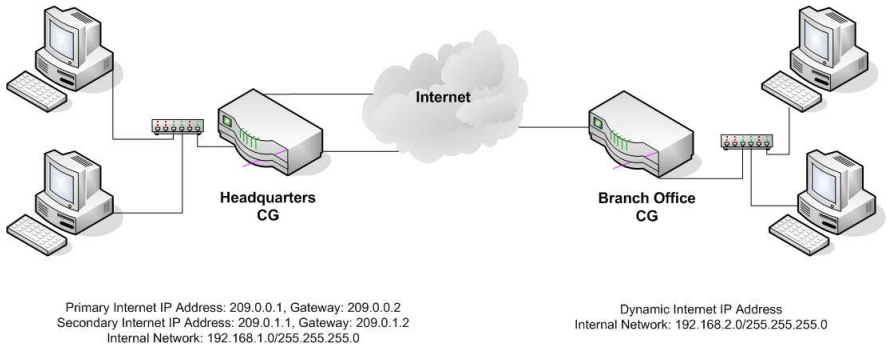
IPSec Failover

Note

SG560, SG565, SG580, SG710 only.

The SG unit can be configured to failover and fallforward between IPSec connections. Two common scenarios are described below.

The following scenario assumes that the Headquarters SG has two static Internet IP addresses and the Branch Office SG has a dynamic Internet IP address. The Branch Office SG establishes an IPSec tunnel to the primary Internet IP address at the Headquarters SG as the primary IPSec tunnel path. If this IPSec connection is detected to have failed, a failover IPSec tunnel is established to the secondary Internet IP address at the Headquarters SG. Once in the failover state, the Branch Office SG will periodically determine if the primary IPSec tunnel path is functioning again, and if so, will fall forward to use the primary link instead.



Setup an IPSec tunnel between the primary Internet IP Addresses (192.168.1.0/24 - 209.0.0.1 <-> 210.0.0.1 – 192.168.2.0/24). Default values are used in the configuration unless otherwise specified below:

Headquarters SG configuration:

Tunnel name: PrimaryLink

Local interface: Internet port

Keying: Aggressive mode (IKE)

Local address: Static IP address

Remote address: Dynamic IP address

Route to remote endpoint: Internet port's gateway

Remote required endpoint ID: primary@branch

Local network: 192.168.1.0/255.255.255.0

Remote network: 192.168.2.0/255.255.255.0

Branch office SG configuration:

Tunnel name: PrimaryLink

Enable this tunnel: Unchecked

Local interface: Default gateway interface

Keying: Aggressive mode (IKE)

Local optional endpoint ID: primary@branch

The remote party's IP address: 209.0.0.1

Local network: 192.168.2.0/255.255.255.0

Remote network: 192.168.1.0/255.255.255.0

Setup an IPSec tunnel between the secondary Internet IP Addresses (192.168.1.0/24 - 209.0.1.1 <-> 210.0.1.1 – 192.168.2.0/24). Default values are used in the configuration unless otherwise specified below:

Headquarters SG configuration:

Tunnel name: SecondaryLink

Local interface: Internet port

Keying: Aggressive mode (IKE)

Local address: Static IP address

Remote address: Dynamic IP address

Route to remote endpoint: DMZ port's gateway

Remote required endpoint ID: secondary@branch

Local network: 192.168.1.0/255.255.255.0

Remote network: 192.168.2.0/255.255.255.0

Branch Office SG configuration:

Tunnel name: SecondaryLink

Enable this tunnel: Unchecked

Local interface: Default gateway interface

Keying: Aggressive mode (IKE)

Local optional endpoint ID: secondary@branch

The remote party's IP address: 209.0.1.1

Local network: 192.168.2.0/255.255.255.0

Setup an unused aliased IP address on the LAN interface of both the Headquarter and Branch Office SGs. For example:

Headquarters SG configuration:

Alias IP address: 192.168.11.1

Alias subnet mask: 24

Branch office SG configuration:

Alias IP address: 192.168.12.1

Alias subnet mask: 24

Setup a Primary Link Test IPSec tunnel between the primary Internet IP Addresses (192.168.11.0/32 - 209.0.0.1 <-> 210.0.0.1 – 192.168.12.0/32). This will be used to determine whether the Primary Link is back up in the failed over state. Default values are used in the configuration unless otherwise specified below:

Headquarters SG configuration:

Tunnel name: PrimaryLinkTest

Local interface: Internet Port

Keying: Aggressive mode (IKE)

Local address: Static IP address

Remote address: Dynamic IP address

Route to remote endpoint: Internet port's gateway

Initiate phase 1 & 2 rekeying: Unchecked

Remote required endpoint ID: primarytest@branch

Phase 1 key lifetime (sec): 7200

Local network: 192.168.11.1/255.255.255.255

Remote network: 192.168.12.1/255.255.255.255

Phase 2 key lifetime (sec): 7200

Branch Office SG configuration:

Tunnel name: PrimaryLinkTest

Enable this tunnel: Unchecked

Local Interface: Default gateway interface

Keying: Aggressive mode (IKE)

Local optional endpoint ID: primarytest@branch

The remote party's IP address: 209.0.0.1

Local network: 192.168.12.1/255.255.255.255

Remote network: 192.168.11.1/255.255.255.255

Manually edit the ifmond.conf on both the Branch Office SG to configure for IPSec failover and fallforward.

```
##-- Custom entries MUST be added below this point
```

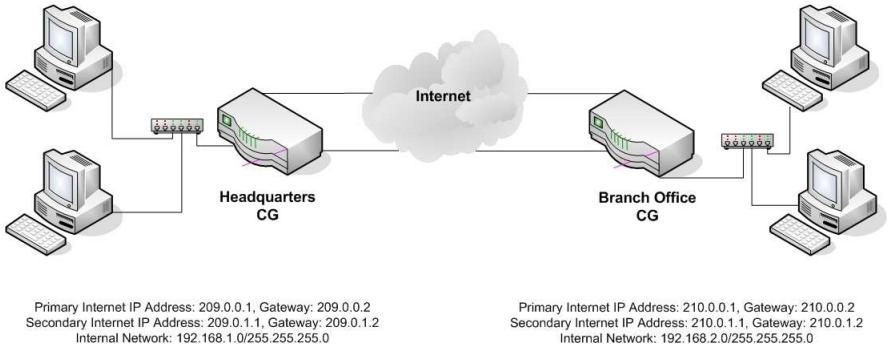
```
connection primarylinktest
   parent     conn-eth1
   start ipsec auto --add PrimaryLinkTest
   start ipsec auto --up PrimaryLinkTest
   stop  ipsec whack --delete --name PrimaryLinkTest
   maximum_retries  2147483647
   retry_delay      5
   test_delay 5
   test  ifretry 2 5 ping -I 192.168.12.1 192.168.11.1 -c 3

connection primarylink
   parent     primarylinktest
   start ipsec auto --add PrimaryLink
   start ipsec auto --up PrimaryLink
   stop  ipsec whack --delete --name PrimaryLink
   maximum_retries  2147483647
   retry_delay      5
   test_delay 5
   test  ifretry 2 5 ping -I 192.168.2.1 192.168.1.1 -c 3

connection secondarylink
   parent     conn-eth1
   start ipsec auto --add SecondaryLink
   start ipsec auto --up SecondaryLink
   stop  ipsec whack --delete --name SecondaryLink
   maximum_retries  2147483647
   retry_delay      5
   test_delay 5
   test  ifretry 2 5 ping -I 192.168.2.1 192.168.1.1 -c 3

service service-ipsec
   group primarylinktest
   group secondarylink
```

The following scenario assumes that the Headquarters SG and Branch Office SG each have two static Internet IP addresses. The Branch Office SG establishes an IPSec tunnel from its primary Internet IP address to the primary Internet IP address at the Headquarters SG as the primary IPSec tunnel path. If this IPSec connection is detected to have failed, a failover IPSec tunnel is established from the secondary Internet IP address to the cecondary Internet IP address at the Headquarters SG. Once in the failover state, the Branch Office SG will periodically determine if the primary IPSec tunnel path is functioning again, and if so, will fallforward to use the primary link instead.



Setup an IPSec tunnel between the primary Internet IP Addresses (209.0.0.1 <-> 210.0.0.1). Default values are used in the configuration unless otherwise specified below:

Headquarters SG configuration:

Tunnel name: PrimaryLink

Local interface: Internet port

Route to remote endpoint: Internet port's gateway

The remote party's IP address: 210.0.0.1

Local network: Address of Internet port

Remote network: Remote endpoint

Branch Office SG configuration:

Tunnel name: PrimaryLink

Local interface: Internet port

Route to remote endpoint: Internet port's gateway

The remote party's IP address: 209.0.0.1

Local network: Address of Internet port

Remote network: Remote endpoint

Setup an IPSec tunnel between the secondary Internet IP Addresses (209.0.1.1 <-> 210.0.1.1). Default values are used in the configuration unless otherwise specified below:

Headquarters SG configuration:

Tunnel name: SecondaryLink

Enable this tunnel: Checked

Local interface: DMZ port

Route to remote endpoint: DMZ port's gateway

The remote party's IP address: 210.0.1.1

Local network: Address of DMZ port

Remote network: Remote endpoint

Branch Office SG configuration:

Tunnel name: SecondaryLink

Enable this tunnel: Checked

Local interface: DMZ port

Route to remote endpoint: DMZ port's gateway

The remote party's IP address: 209.0.1.1

Local network: Address of DMZ port

Remote network: Remote endpoint

Setup corresponding GRE tunnels over the IPSec tunnels configured in steps 1 and 2 (209.0.0.1 <-> 210.0.0.1 and 209.0.1.1 <-> 210.0.1.1). Default values are used in the configuration unless otherwise specified below:

Headquarters SG configuration:

GRE tunnel for primary link:

GRE tunnel name: PrimaryLink

Remote address: 210.0.0.1

Local address: 209.0.0.1

Firewall class: LAN

GRE tunnel for secondary link:

GRE tunnel name: SecondaryLink

Remote address: 210.0.1.1

Local address: 209.0.1.1

Firewall class: LAN

Branch Office SG configuration:

GRE tunnel for primary link:

GRE tunnel name: PrimaryLink

Remote address: 209.0.0.1

Local address: 210.0.0.1

Firewall class: LAN

GRE tunnel for secondary link:

GRE tunnel name: SecondaryLink

Remote address: 209.0.1.1

Local address: 210.0.1.1

Firewall class: LAN

Manually edit the ifmond.conf on both the Headquarter and Branch Office SG to configure for IPSec failover and fallforward.

Headquarters SG ifmond.conf:

```
##-- Custom entries MUST be added below this point
connection primary_route
   parent     primary_ping
   start route add -net 192.168.2.0 netmask 255.255.255.0 dev
gre1
   stop  route del -net 192.168.2.0 netmask 255.255.255.0 dev
gre1
   maximum_retries  2147483647
   retry_delay      5
   test_delay 5
```

```
connection secondary_route
   parent     secondary_ping
   start route add -net 192.168.2.0 netmask 255.255.255.0 dev
gre2
   stop  route del -net 192.168.2.0 netmask 255.255.255.0 dev
gre2
   maximum_retries  2147483647
   retry_delay      5
   test_delay 5


connection primary_ping
   parent     conn-gre1
   maximum_retries  2147483647
   retry_delay      5
   test_delay 5
   test  ifretry 2 5 ping -I 209.0.0.1 210.0.0.1 -c 3


connection secondary_ping
   parent     conn-gre2
   maximum_retries  2147483647
   retry_delay      5
   test_delay 5
   test  ifretry 2 5 ping -I 209.0.1.1 210.0.1.1 -c 3


service service-ipsec
   group primary_ping
   group secondary_ping
```

Branch Office SG ifmond.conf:

```
##-- Custom entries MUST be added below this point
connection primary_route
   parent     primary_ping
   start route add -net 192.168.1.0 netmask 255.255.255.0 dev
gre1
```

```
   stop  route del -net 192.168.1.0 netmask 255.255.255.0 dev
gre1
   maximum_retries  2147483647
   retry_delay      5
   test_delay 5


connection secondary_route
   parent     secondary_ping
   start route add -net 192.168.1.0 netmask 255.255.255.0 dev
gre2
   stop  route del -net 192.168.1.0 netmask 255.255.255.0 dev
gre2
   maximum_retries  2147483647
   retry_delay      5
   test_delay 5


connection primary_ping
   parent     conn-gre1
   maximum_retries  2147483647
   retry_delay      5
   test_delay 5
   test  ifretry 2 5 ping -I 210.0.0.1 209.0.0.1 -c 3


connection secondary_ping
   parent     conn-gre2
   maximum_retries  2147483647
   retry_delay      5
   test_delay 5
   test  ifretry 2 5 ping -I 210.0.1.1 209.0.1.1 -c 3


service service-ipsec
   group primary_ping
   group secondary_ping
```

IPSec Troubleshooting

- **Symptom:** IPSec is not running and is enabled.

  Possible Cause: The SG unit has not been assigned a default gateway.

  Solution: Ensure the SG unit has a default gateway by configuring the Internet connection on the Connect to Internet page or assigning a default gateway on the IP Configuration page.

- **Symptom:** Tunnel is always down even though IPSec is running and the tunnel is enabled.

  Possible Cause: The tunnel is using Manual Keying and the encryption and/or authentication keys are incorrect.

  The tunnel is using Manual Keying and the SG unit's and/or remote party's keys do not correspond to the Cipher and Hash specified.

  Solution: Configure a correct set of encryption and/or authentication keys. Select the appropriate Cipher and Hash that the key have been generated from, or change the keys used to use the selected Cipher and Hash.

- **Symptom:** Tunnel is always Negotiating Phase 1.

  Possible Cause: The remote party does not have an Internet IP address (a *No route to host* message is reported in the system log).

  The remote party has IPSec disabled (a *Connection refused* message is reported in the system log).

  The remote party does not have a tunnel configured correctly because:

  - The tunnel has not been configured.
  - The Phase 1 proposals do not match.
  - The secrets do not match.
  - The RSA key signatures have been incorrectly configured.
  - The Distinguished Name of the remote party has not be configured correctly.
  - The Endpoint IDs do not match.
  - The remote IP address or DNS hostname has been incorrectly entered.
  - The certificates do not authenticate correctly against the CA certificate.

  Solution: Ensure that the tunnel settings for the SG unit and the remote party are configured correctly. Also ensure that both have IPSec enabled and have Internet IP addresses. Check that the CA has signed the certificates.

- **Symptom:** Tunnel is always Negotiating Phase 2

  Possible Cause: The Phase 2 proposals set for the SG unit and the remote party do not match.

  The local and remote subnets do not match.

Solution: Ensure that the tunnel settings for the SG unit and the remote party are configured correctly.

- **Symptom:** The tunnel appears to be up and I can ping across it, but HTTP, FTP, SSH, telnet, etc. don't work

  Possible Cause: The MTU of the IPSec interface is too large.

  Solution: Reduce the MTU of the IPSec interface.

- **Symptom:** Tunnel goes down after a while

  Possible Cause: The remote party has gone down.

  The remote party has disabled IPSec.

  The remote party has disabled the tunnel.

  The tunnel on the SG unit has been configured not to rekey the tunnel.

  The remote party is not rekeying correctly with the SG unit.

  Solution: Confirm that the remote party has IPSec and the tunnel enabled and has an Internet IP address. Ensure that the SG unit has rekeying enabled. If the tunnel still goes down after a period of time, it may be due to the SG unit and remote party not recognising the need to renegotiate the tunnel. This situation arises when the remote party is configured to accept incoming tunnel connections (as opposed to initiate tunnel connections) and reboots. The tunnel has no ability to let the other party know that a tunnel renegotiation is required. This is an inherent drawback to the IPSec protocol. Different vendors have implemented their own proprietry method to support the ability to detect whether to renegotiate the tunnel. Dead peer detection has been implemented based on the draft produced by Cisco Systems (*draft-ietf-ipsec-dpd-00.txt*). Unfortunately, unless the remote party implements this draft, the only method to renegotiate the tunnel is to reduce the key lifetimes for Phase 1 and Phase 2 for Automatic Keying (IKE). This does not occur for Manual Keying.

- **Symptom:** Dead Peer Detection does not seem to be working

  Possible Cause: The tunnel has Dead Peer Detection disabled.

  The remote party does not support Dead Peer Detection according to *draft-ietf-ipsec-dpd-00.txt*

  Solution: Enable Dead Peer Detection support for the tunnel. Do not use Dead Peer Detection if the remote party does not support *draft-ietf-ipsec-dpd-00.txt*.

- **Symptom:** Tunnels using x.509 certificate authentication do not work

  Possible Cause: The date and time settings on the SG unit has not been configured correctly.

  The certificates have expired.

  The Distinguished Name of the remote party has not be configured correctly on the SG unit's tunnel.

  The certificates do not authenticate correctly against the CA certificate.

The remote party's settings are incorrect.

Solution: Confirm that the certificates are valid. Confirm also that the remote party's tunnel settings are correct. Check the Distinguished Name entry in the the SG unit's tunnel configuration is correct.

- **Symptom:** Remote hosts can be accessed using IP address but not by name

  Possible cause: Windows network browsing broadcasts are not being transmitted through the tunnel.

  Solution: Set up a WINS server and use it to have the remote hosts resolve names to IP addresses.

  Set up LMHOST files on remote hosts to resolve names to IP adresses.

- **Symptom:** Tunnel comes up but the application does not work across the tunnel.

  Possible cause: There may be a firewall device blocking IPSec packets.

  The MTU of the IPSec interface may be too large.

  The application uses broadcasts packets to work.

  Solution: Confirm that the problem is the VPN tunnel and not the application being run. These are the steps you can try to find where the problem is (it is assumed that a network to network VPN is being used):

  Ping from your PC to the Internet IP address of the remote party (it assumed that the remote party is configured to accept incoming pings)

  Ping from your PC to the LAN IP address of the remote party.

  Ping from your PC to a PC on the LAN behind the remote party that the tunnel has been configured to combine.

  If you cannot ping the Internet IP address of the remote party, either the remote party is not online or your computer does not have its default gateway as the SG unit. If you can ping the Internet IP address of the remote party but not the LAN IP address, then the remote party's LAN IP address or its default gateway has not been configured properly. Also check your network configuration for any devices filtering IPSec packets (protocol 50) and whether your Internet Service Provider is filtering IPSec packets. If you can ping the LAN IP address of the remote party but not a host on the remote network, then either the local and/or remote subnets of the tunnel settings have been misconfigured or the remote host does not have its default gateway as the remote party.

  If you can ping across the tunnel, then check if the MTU of the IPSec interface is allowing packets to go through. Reduce the MTU if large packets are not being sent through the tunnel.

  If the application is still not working across the tunnel, then the problem is with the application. Check that the application uses IP and does not use broadcast packets since these are not sent across the IPSec tunnels. You should contact the producer of the application for support.

Port Tunnels

Port tunnels are point to point tunnels similar to regular VPNs, but only offer transport for a TCP service from one end of the tunnel to the other. This allows you to “wrap” a TCP service, such as telnet or mail retrieval (POP3), in an HTTP or SSL connection. Note that a single port tunnel may transport a single TCP port only.

The SG unit supports two kinds of port tunnels.

HTTP Tunnels are port tunnels that send data using the HTTP protocol, and are not encrypted. HTTP tunnels are *not* encrypted. They can be useful when the SG unit is behind a firewall that only allows outgoing HTTP connections and blocks all other traffic.

SSL Tunnels are port tunnels that send data using an encrypted SSL pipe. In order to use an SSL tunnel, you must first install an SSL certificate using the **Upload SSL Certificates** page or the **Create SSL Certificates** page; see the *Upload SSL certificates* and *Create SSL certificates* sections of the chapter entitled *Firewall*. SSL tunnels can be useful for encrypting TCP services that are by themselves unencrypted, such as a telnet or FTP session.

The end of the port tunnel that is offering the TCP service (such as a telnet or FTP server) must be configured as a **Tunnel Server**. The end of the port tunnel that is accessing the TCP service must be configured as a **Tunnel Client**.

Tunnel server

A tunnel server accepts connections on **Tunnel Port** from a host on the Internet, and forwards them over the **Data Port** to the **Data Server**.

Click **Port Tunnels** from the **VPN** section of the main menu. Select either **HTTP Tunnel Server** or **SSL Tunnel Server** and click **Add**.

Enter a descriptive **Name** for this tunnel server. Check **Enable**.

In **Data Server**, enter the IP address of the local server that is offering the TCP service, such as a local mail or FTP server. In **Data Port**, enter the port on which the TCP service is running. Incoming requests from hosts on the remote end of the tunnel are forwarded to this IP address and port.

In **Tunnel Port**, Enter the TCP port on which to listen for connections from the client. This must match the tunnel client’s **Tunnel Port**.

- The following fields are displayed for **HTTP Tunnel Server** only:

If necessary, you may specify the **Content Length** to use in HTTP PUT requests. You may also set **Strict Content Length** to force this **Content Length** for all requests.

You may specify a **Maximum Age** for connections, after which the connection is closed, and a **Keep Alive** interval, the interval at which to send keep alive bytes to keep the connection open.

- The following field is displayed for **SSL Tunnel Server** only:

  You may specify the **Protocol** to use when negotiating the SSL connection. Leave this set to **Raw** when incoming connections are from a tunnel client. Setting **Protocol** to another value allows the tunnel server to accept connections directly from an SSL client other than a tunnel client, e.g. a mail client configured to use **POP3** over SSL.

Tunnel client

A tunnel client accepts connections on **Data Port** from a host on the local network, and forwards them over the **Tunnel Port** to the **Tunnel Server**.

Click **Port Tunnels** from the **VPN** section of the main menu. Select either **HTTP Tunnel Client** or **SSL Tunnel Client** and click **Add**.

Enter a descriptive **Name** for this tunnel client. Check **Enable**.

In **Data Port**, enter the TCP port on which to listen for connections from local hosts to forward across the tunnel. It is not necessary for this to match the tunnel server's **Data Port**, but it often will.

Enter the publically accessible IP address of the remote **Tunnel Server**, and in **Tunnel Port**, enter the TCP port on which the tunnel server is listening for connections. This must match the tunnel server's **Tunnel Port**.

- The following fields are displayed for **HTTP Tunnel Client** only:

  If necessary, you may specify the **Content Length** to use in HTTP PUT requests. You may also set **Strict Content Length** to force this **Content Length** for all requests.

  You may specify a **Maximum Age** for connections, after which the connection is closed, and a **Keep Alive** interval, the interval at which to send keep alive bytes to keep the connection open.

  You may disregard the remaining fields if you are not connecting to the HTTP tunnel server via an HTTP **Proxy Server**.

Otherwise, either the **Proxy Server** IP address and the **Proxy Port**. If the proxy server requires authentication, enter the details in **Proxy Username** and **Proxy Password**.

If the proxy accepts connects from clients with a specific User Agent field only, enter it in **Proxy User Agent**.

If the HTTP proxy is a buffering proxy, then enter the **Proxy Buffer Size**. Otherwise set this field to 0. You may also specific the timeout before sending padding to fill up the buffer size in **Proxy Padding Timeout**.

- The following field is displayed for **SSL Tunnel Server** only:

  You may specify the **Protocol** to use when negotiating the SSL connection. Leave this set to **Raw** connecting to a tunnel server. Setting **Protocol** to another value allows the tunnel client to connect directly to an SSL server other than a tunnel server, e.g. a mail server configured to use **POP3** over SSL.

6. USB

Note

SG565 only.

The SG565 has two USB (Universal Serial Bus) ports to which you can attach USB storage devices (e.g. hard drives, flash drives, card readers), USB printers, USB network devices and USB narrowband (non-DSL) modems. A USB hub may be used if you need to attach more than two USB devices simultaneously.

Note

USB DSL modems are not supported at this time.

The following walks you through configuring your SG unit to use the aforementioned USB devices, and how to share printers and network attached storage with a Windows network.

Attach the USB device

Ensure that the USB device is connected using a USB cable and that the device is powered on. Some USB devices, such as USB flash drives, draw their power directly from the USB port, others may require a separate power adapter.

USB Mass Storage Devices

USB mass storage devices can be attached to the SG unit for use as a print spool or to share with your Windows network as a network attached storage device (NAS). A typical use for NAS is for using the SG unit as a network file server.

USB mass storage devices include USB flash drives and keychains, USB flash card readers loaded with flash cards, USB hard drives, and certain digital cameras and portable music players.

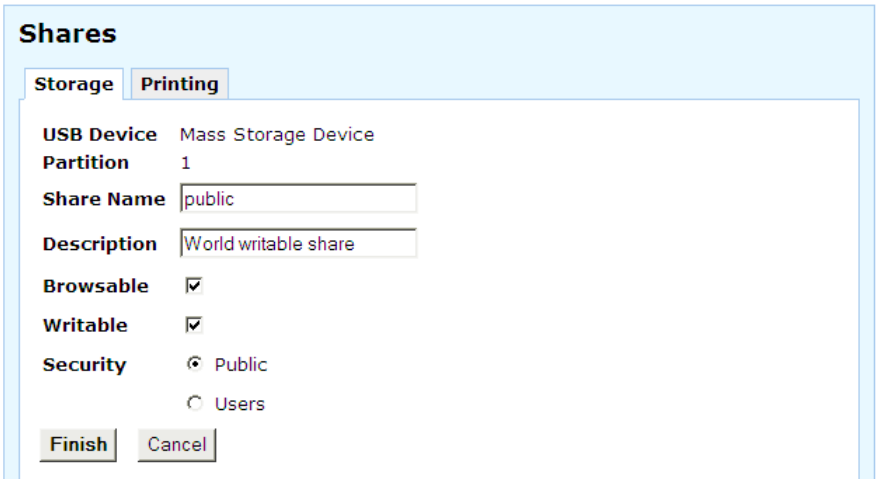
This section describes how to set up the SG unit for network attached storage. For information on using a USB mass storage device as a print spool, refer to the *USB Printers* section.

Share the storage device

Select **Shares** from the **Networking** section of the main menu. Click the **Storage** tab.

All **USB Devices** or device **Partition**s that are available to share are listed along with their **Size**s and for previously configured shares, their **Share Name**s.

Locate the **USB Device** or device **Partition** that you want to share and click its **Edit** icon.

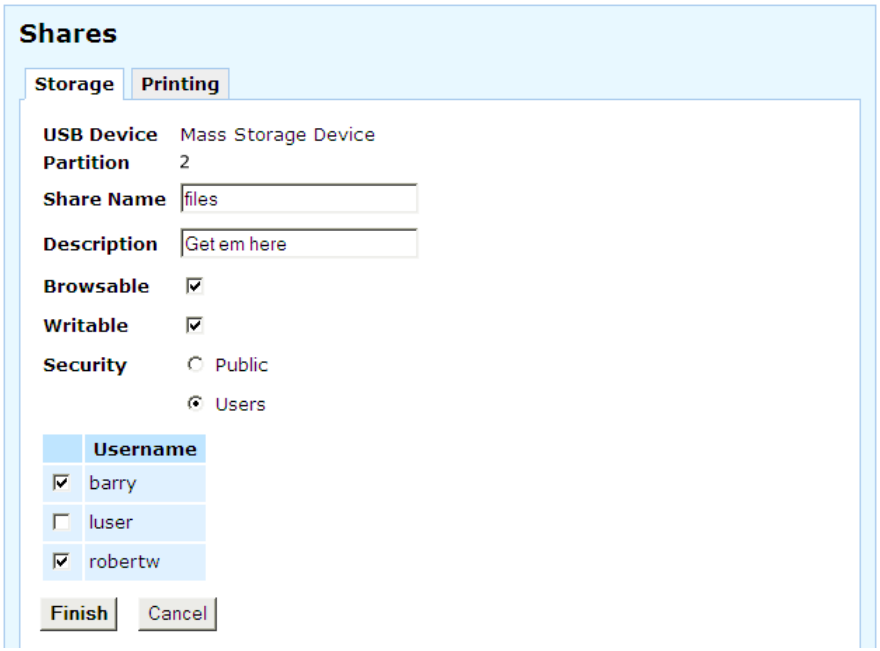


Enter a **Share Name**, this is the name that is displayed when browsing your Windows workgroup or domain.

Enter a **Description** (optional).

Set access permissions

The remaining settings control access to the network share from your LAN.



Browsable: Display an icon for the network when browsing the network from a Windows PC. To access the network share when this is unchecked, the user must manually enter the address in the address bar (e.g. *SG565**public*\).

Writable: The network share is writable, i.e. users can modify and create new files.

Public: A login and password is not required to access the network share.

Users: A valid login and password is required to access the network share. Selecting this option displays a list of users. Check the boxes next to the users to whom you wish to grant access.

Note

See the Users *section in the chapter entitled* System *for information on adding new users.*

Click **Finish**.

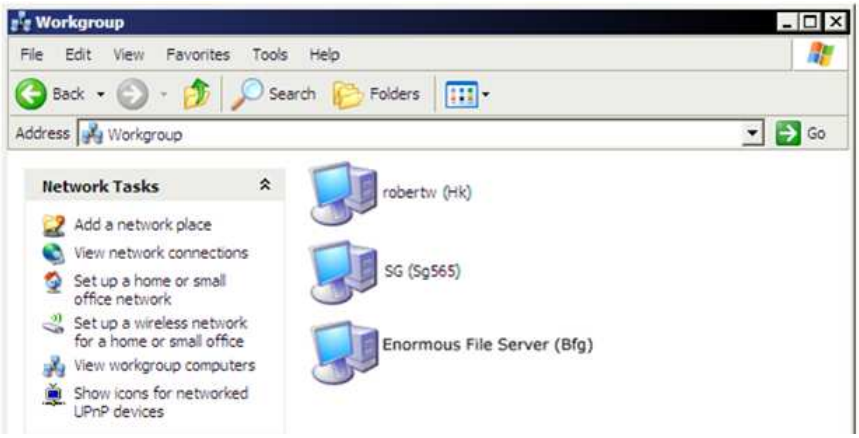
Once configured, you may enable and disable network shares under the **Storage** tab using the **Enable**/**Disable** checkbox.

Join a Windows workgroup

The next step is to configure your SG unit to join your Window workgroup or domain. Select **Network Setup** from the **Networking** menu. Click the **Advanced** tab.

Under the **Unit Workgroup** heading, enter the name of your Windows workgroup or domain and click **Apply**. Typically, this name is UPPERCASE.

Once NAS devices or printers have been shared, your SG unit becomes visible to other members.



To test this, browse the workgroup from a Windows PC that is a workgroup member. In Windows XP, open **My Network Places** and under **Network Tasks** on the left, click **View workgroup computers** to browse the workgroup.

Note

Setting up your Windows workgroup or domain is beyond the scope of this manual. Refer to the documentation shipped with Windows, or the Microsoft website for further information.

Partitioning a USB mass storage device

Warning

This procedure is intended for experts and power users only.

The standard Linux command line tools are present on the SG unit for partitioning (*fdisk*) and creating filesystems (*mkfs*) on an attached USB mass storage device. Alternatively, you may use the standard Windows tools or a third party utility such as PartitionMagic to partition a USB mass storage device before attaching it to the SG unit.

This section contains an example walkthrough of partitioning a USB mass storage device using the SG unit. The following example splits a 128MB USB mass storage device into two equally sized partitions.

Warning

Repartitioning a device causes all data on that device to be lost. Back up any data before proceeding.

Attach the USB mass storage device. After 10 – 15 seconds, select **Advanced** from the **System** menu and click **System Log**. Look for lines similar to the following to see which device name is has been assigned.

```
Apr 22 01:19:49 klogd: USB Mass Storage device found at 4

Apr 22 01:20:58 klogd: SCSI device sda: 256000 512-byte hdwr
sectors (131 MB)
```

In this case, the device name is *sda*. If there is a single USB mass storage device attached, it is typically be assigned *sda*, otherwise it may by *sdb*, *sdc*, etc.

telnet or *ssh* to the SG unit and log in. Run the *fdisk* command with the argument */dev/<device name>*, e.g.

```
fdisk /dev/sda
```

Type **p** to display the partition table.

```
Command (m for help): p

Disk /dev/sda: 5 heads, 50 sectors, 1024 cylinders

Units = cylinders of 250 * 512 bytes

   Device Boot    Start       End    Blocks   Id  System

/dev/sda1             1      1024    127975    b  Win95 FAT32
```

Delete any existing partitions by typing **d** the entering the partition number, e.g. enter **1** to delete */dev/sda1*.

Create a new partition by typing **n** then **p** for *primary*, then the partition number.

Note

The SG unit support primary partitions only, so you are limited to four partitions.

Enter the cylinder for the partition to start on, generally the default is fine. Enter the cylinder for the partition to end on, or a size for the partition with *+(size in mb)M*.

```
Command (m for help): n

Command action

   e   extended

   p   primary partition (1-4)

p

Partition number (1-4): 1

First cylinder (1-1024, default 1):

Using default value 1

Last cylinder or +size or +sizeM or +sizeK (1-1024, default
1024): +64M
```

Repeat the process for each partition to want to create. For the last partition, the default last cylinder is generally be fine.

```
Command (m for help): n

Command action

   e   extended

   p   primary partition (1-4)

p

Partition number (1-4): 2

First cylinder (526-1024, default 526):

Using default value 526

Last cylinder or +size or +sizeM or +sizeK (526-1024, default
1024):

Using default value 1024
```

For each partition, set the partition type to match the type of filesystem you are going to create on it by typing **t**, the partition number, then the type code (**L** to view type codes). In this example, we are creating FAT32 partitions (type code **b**).

```
Command (m for help): t

Partition number (1-4): 1

Hex code (type L to list codes): b

Changed system type of partition 1 to b (Win95 FAT32)
```

Type **w** to save your changes to the partition table. From the web management console, select **Advanced** from the **System** menu, and click **Reboot**.

telnet or *ssh* to the SG unit and log in. For each partition, run the appropriate *mkfs* command. To create FAT32 on our two example partitions, we use:

```
mkfs.vfat –F 32 /dev/sda1
```

then

```
mkfs.vfat –F 32 /dev/sda2
```

From the web management console, select **Advanced** from the **System** menu, and click **Reboot**. The partitions are now ready to use.

USB Printers

The SG unit's print server allows you to share attached USB printers with your LAN. After the printer server has been configured, the SG unit and printer are displayed when you browse your Windows workgroup or domain.

Mac OSX, Linux and other UNIX-based or UNIX-like machines on the network can use the *LPR* / *LPD* protocol for remote printing.

This section describes how to configure the SG565 to share a USB printer, and how to set up remote printing on a Windows PC.

Warning

Many inexpensive printers do not work with the SG's Print Server, as their drivers expect the printer to be attached directly to the PC you are printing from, or the printer itself relies on utilizing the PC's CPU for processing print jobs (host-based/GDI printers). Due to these technical limitations, we simply cannot support these types of printers.

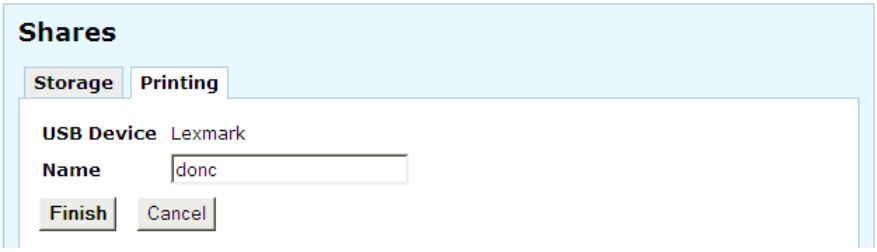
It is therefore strongly recommended that you use a business grade printer with the SG's print server. *Non-business grade printers may work, but we are unable to provide support if they do not; see the* Troubleshooting *section at the end of this chapter for suggestions.*

Additionally, advanced features such as cartridge status reporting may not function correctly. Multifunction and all-in-one printers are not supported.

Set up the print server

Attach the USB printer to the SG.

Select **Shares** from the **Networking** section of the main menu. Click the **Printing** tab. Locate the printer to share and click its **Edit** icon.



Enter a short descriptive **Name** for the printer. This is the name that is displayed when browsing your Windows workgroup or domain, and the name of the queue for *LPR / LPD* connections. Click **Finish**.

Set up the print spool

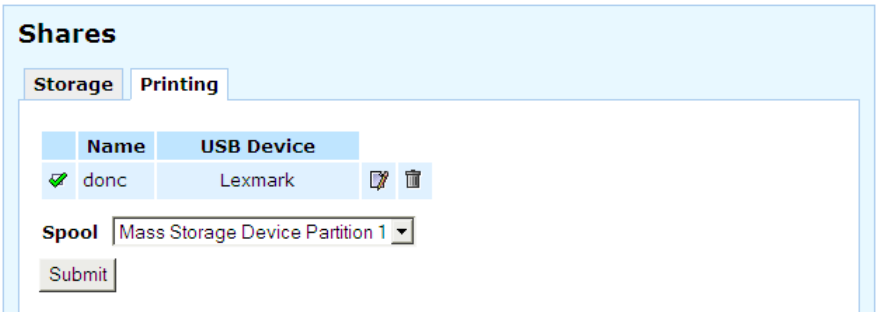
By default, the SG unit spools incoming print jobs into memory (RAM) before sending them to the printer. This can be an issue if you have many services running on the SG unit (e.g. many VPN connections, Intrusion Detection, Web Cache, etc.) and it is low on memory, or you are intending to print large documents or images.

When a Windows PC sends a document or image to the printer attached to the SG unit, it first converts it into a format that the printer can read. The resulting file that the SG unit has to store in memory can be many times larger than the size of the original document or image.

Note

To avoid the SG running out of RAM and print jobs failing, we recommend that you use a USB mass storage device to spool print jobs.

If you wish to spool to memory or set up the spool later, proceed to *Set up Windows PCs for remote printing*.



Otherwise, attach the USB mass storage device and select the device or device partition on which to store the print spool from the **Spool** pull down menu under the **Printing** tab.

Note

You may simultaneously use a USB mass storage device or device partition as a print spool and a Network Attached Storage device. However, the spool directory becomes visible (as spool*) and there is a higher chance of the device filling up, causing print jobs to fail. For these reasons, we recommend dedicating a partition or device for use as the print spool.*

For information on partitioning a USB mass storage device, refer to the USB Mass Storage Devices *section earlier in this chapter.*

Join a Windows workgroup

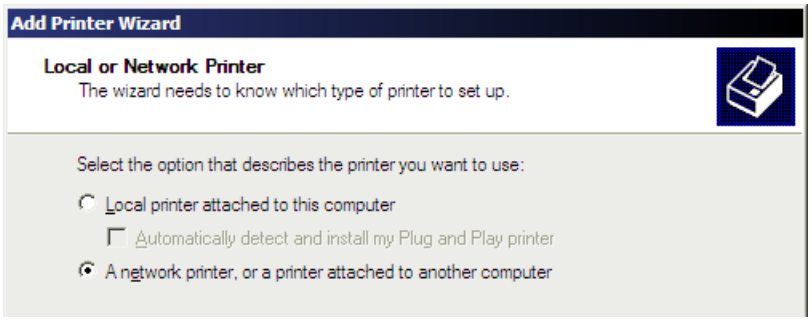
Follow the step under *Join a Windows workgroup* in the *USB Mass Storage Devices* section earlier in this chapter.

Set up Windows PCs for remote printing

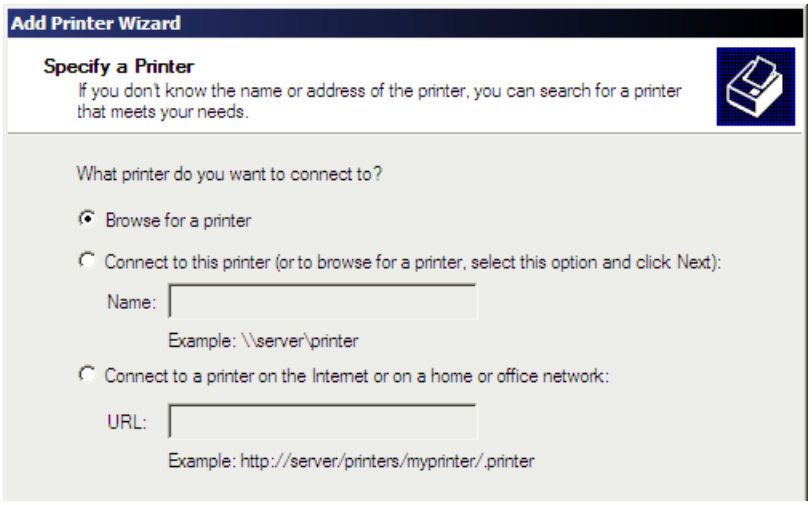
Repeat the following steps for each Windows PC to be enabled for remote printing. These steps are for Windows XP, steps are similar for Windows 2000 and 95/98.

Click **Start** -> (**Settings**) -> **Printers and Faxes**. Under **Printer Tasks** on the left, click **Add a printer**.

The **Add Printer Wizard** is displayed. Click **Next**.


Add Printer Wizard
Local or Network Printer
The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Local printer attached to this computer
Automatically detect and install my Plug and Play printer
A network printer, or a printer attached to another computer

Select **A network printer, or a printer attached to another computer** and click **Next**.

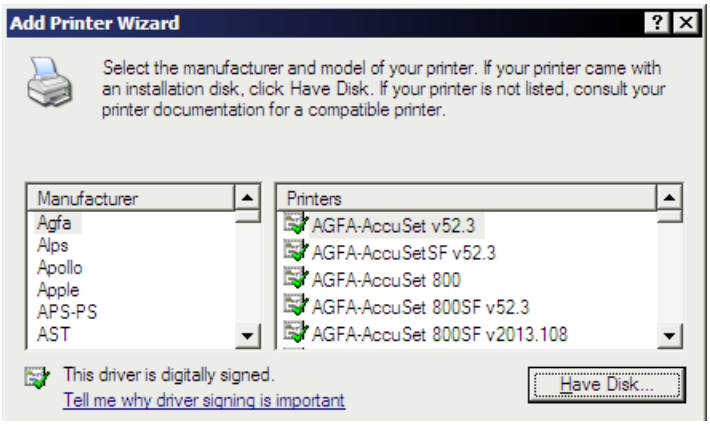

Add Printer Wizard
Specify a Printer
If you don't know the name or address of the printer, you can search for a printer that meets your needs.
What printer do you want to connect to?
Browse for a printer
Connect to this printer (or to browse for a printer, select this option and click Next):
Name:
Example: \\server\printer
Connect to a printer on the Internet or on a home or office network:
URL:
Example: http://server/printers/myprinter/.printer

Select **Browse for a printer** and click **Next**.

Locate the SG unit by expanding your Windows workgroup and locating the SG by its hostname. The hostname is set on the SG unit under **Network Setup** -> **Advanced** -> **Unit Hostname**. Select the printer and click **Next**.

You may receive a warning about the SG unit automatically installing print drivers on your PC. Ignore it, the SG does not install print drivers automatically.

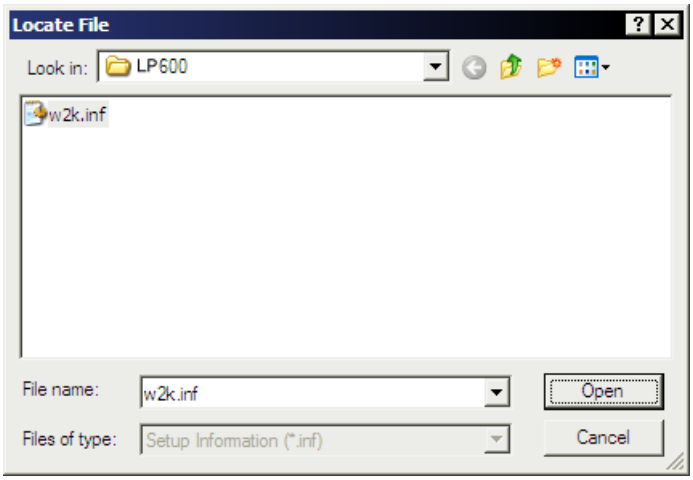
If a dialog is displayed to inform you that no appropriate print driver could be found on the SG unit, click **OK**.



Select the appropriate driver for your printer.

If an appropriate printer driver is not already installed on the Windows PC, insert the floppy disk or CD that shipped with your printer, or download the appropriate drivers from the manufacturer's website (you may have to extract this if it is in a compressed archive or *.exe* format).

Click **Have Disk**. Enter the location of the print drivers in **Copy manufacturer's files from** (e.g. *A:* for a floppy or *D:* for a CD, or the locate where you downloaded or extracted the drivers) and click **Browse**.



Locate the *.inf* file for your printer and click **Open** then **OK**.

Add Printer Wizard
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.
Printers
Lexson P600 Series
This driver is digitally signed.
Tell me why driver signing is important
Have Disk...
OK
Cancel

Select your printer model and click **OK**.

If your printer model is not listed, click **Have Disk** and **Browse** again. Drivers for several different printers and different operating systems are often distributed together by the manufacturer, so there may by several different *.inf* files.

Follow the onscreen instructions to install the printer driver. This varies from printer to printer.

Note

If you cannot locate the appropriate .inf file or the printer driver fails to install, see Print driver installation fails in the Printer Troubleshooting section.

Choose whether to use this printer as the default printer for this Windows PC and click **Next**. Click **Finish**.

To test the printer, printing a simple text document from Notepad, or right click the printer in **Printers and Faxes**, click **Properties** then click **Print Test Page**.

LPR / LPD setup

> ***Note***
>
> *This information is generally not relevant for Windows network environments.*

Once the print server has been set up, the SG unit also listen on the standard LPR / LPD network port (TCP 515) for incoming print jobs.

Set up your LPR client to print to a remote LPD queue as specified by your operating system's documentation. The queue name is the **Name** you specified during *Set up print server*.

Printer Troubleshooting

This section lists some common issues and steps you can take to resolve them.

If none of these address your issue, consult the SG Knowledge Base at: http://www.cyberguard.com/snapgear/knowledgebase.html

The Knowledge Base also contains information on getting specific printers to interoperate with the SG's print server.

Print driver installation fails

If you are unable to install the remote printer, attach it directly to the Windows PC and follow the manufacturer's instructions to install it as if it were a local printer.

Once the printer has installed, reconnect it to the SG unit and follow the instructions from the *Set up print server* section onwards. When you are prompted to select the print driver in the *Add Printer Wizard*, the driver for your printer should now be listed under the manufacturer.

After the wizard has completed, you may delete the local printer.

Printer shows up in *Printers and Faxes*, but printing fails

Some printers may require you to disable advanced printing features and/or bidirectional support.

Disable **Advanced Printing Features** by clicking **Control Panel** -> **Printers and Faxes** -> right click printer -> **Properties** -> **Advanced** -> and uncheck **Enable Advanced Printing Features**.

Disable **Bidirectional Support** by clicking **Control Panel** -> **Printers and Faxes** -> right click printer -> **Properties** -> **Ports** -> and uncheck **Enable Bidirectional Support**.

Printing still fails

Here are a few more troubleshooting suggestions:

- Check whether you can print a single page from *Notepad* (**Start** -> **Programs** -> **Accessories** -> **Notepad**). If this works, it is possible your print spool is too small.
- Ensure you are using the correct drivers and that the printer is functioning correctly by attaching the printer to a PC, installing it as per the manufacturer's instructions and printing a test page.
- Download the latest drivers from the manufacturer's web site.
- Consult the SG Knowledge Base which may contain specific information on getting your printer to interoperate with the SG unit. The Knowledge Base is online at: http://www.cyberguard.com/snapgear/knowledgebase.html
- Search the web for other people's experiences using this printer with other print servers. If it does not work with other print servers, it will not work with the SG unit's printer server either. A good resource is online at: http://www.ozcableguy.com/usb_print.html
- If none of these suggestions are helpful and your printer is business grade and *not* host-based, lodge a support request with SG technical support: http://www.cyberguard.com/support/online_support/sg/index.html

USB Network Devices and Modems

Once your USB network device or modem has been attached and the appropriate driver loaded (see the *Attach the USB device* section towards the start of this chapter), it appears in **Network Setup** under the **Networking** menu. See the chapter entitled *Network Setup* for possible configurations.

7. System

Date and Time

We recommend setting the SG unit's clock to the correct date and time, otherwise system log message time stamps do not match the time of the event. If you are using certificates for SSL or IPSec, it is especially important that you set the date and time correctly, as all certificates include an expiry date after which they do not function.

Set date and time

If you have a Javascript enabled web browser, click the top **Set Date and Time** button to synchronize the time on the SG unit with that of your PC.

You may also set the date and time manually by selecting the **Year**, **Month**, **Date**, **Hour** and **Minute** and clicking the bottom **Set Date and Time** button.

NTP time server

The SG unit can synchronize its system time with a remote time server using the Network Time Protocol (NTP). Configuring the NTP time server ensures that the SG unit's clock is accurate soon after the Internet connection is established.

To set the system time using NTP, select the **Set Time** checkbox on the **NTP Server Configuration** page and enter the IP address of the time server in the **Remote NTP Server** field.

Note

*When synchronizing with an NTP server, the date and time is displayed in UTC. To display local time, you must set the **Locality** appropriately.*

Locality

Select your local **Region** and click **Submit**. The system clock subsequently displays local time. By default, the system clock displays UTC.

Backup/Restore Configuration

In the unlikely event that your SG unit should lose its configuration, or if it should require a factory reset, configuration stored on a PC, USB storage device, or some other safe place can be restored to minimize downtime.

A copy of your current configuration can also be stored on the SG unit itself. This is useful for storing multiple configuration profiles, or as a quick snapshot of the “known good” configuration before configuration changes are made that may causes the unit to stop functioning as before.

Configuration may also be saved remotely as a plain, unencrypted text file.

After configuring your SG unit it is strongly recommended that you remotely back up your configuration to an encrypted file.

Note

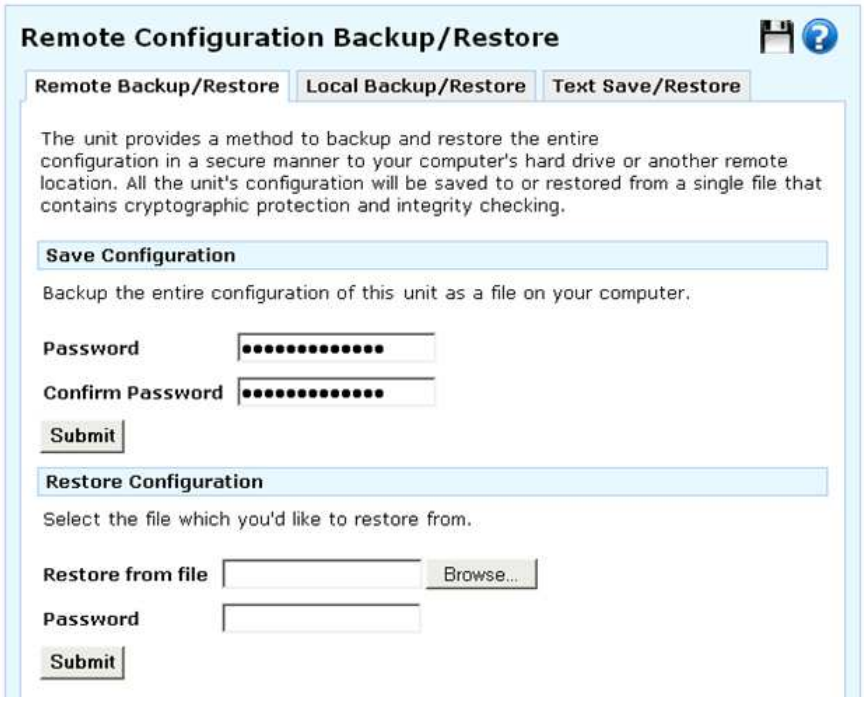
It is good practice to perform remote configuration back ups regularly.

Locally stored configurations are erased by factory resets, and will become unretrievable should the SG unit become uncontactable. Therefore they should not be considered a substitute for performing regular, remote configuration back ups.

Select **Backup/Restore** from the **System** section of the main menu, or the black backup/restore icon at the top right hand side of the screen.

Remote backup/restore

Click the **Remote backup/restore** tab.


Remote Configuration Backup/Restore
Remote Backup/Restore
Local Backup/Restore
Text Save/Restore
The unit provides a method to backup and restore the entire configuration in a secure manner to your computer's hard drive or another remote location. All the unit's configuration will be saved to or restored from a single file that contains cryptographic protection and integrity checking.
Save Configuration
Backup the entire configuration of this unit as a file on your computer.
Password
Confirm Password
Submit
Restore Configuration
Select the file which you'd like to restore from.
Restore from file
Browse...
Password
Submit

To back up your configuration, enter and confirm a **Password** with which to protect this file and click **Submit**. Save the file in a safe place.

Note

Ensure this is a hard to guess password, as all passwords including IPSec passwords and private keys are downloaded into your saved configuration. Ensure your password is easy to remember, if this password is lost there is no way to restore your configuration.

To restore configuration, click **Browse** to locate the *.sgc* configuration file you previously backed up, enter its **Password** and click **Submit**.

Local backup/restore

Click the **Local backup/restore** tab.

Enter a **Description** for this configuration. It is not necessary to include the time and date in the description, they are recorded automatically.

Note

Each configuration snapshot stores a single configuration only, existing configuration snapshots on the SG unit are not *saved inside any subsequent snapshots.*

Restore locally backed up configurations by click its corresponding **Restore** icon in the **Restore or Delete Configuration**. Restoring a remote or local configuration snapshot will not remove existing local configuration snapshots. They must be removed manually by clicking the corresponding **Delete** icon in the **Restore or Delete Configuration** table. You will be prompted to confirm either of these actions.

Text save/restore

Click the **Text save/restore** tab.

Copy and paste the configuration files to and from a plain text file stored on a PC for backup purposes. Click **Submit** and **Reboot** to apply any changes.

Warning

Passwords are stored unencrypted, and plain text files are prone to undetected corruption. It is therefore preferable to use ***Remote backup/restore*** *for regular backups.*

Users

This section details adding administrative users, as well as local users for PPTP, L2TP or dialin access, or access through the access control web proxy (see the *Access Control* section in the chapter entitled *Firewall*).

Administrative users

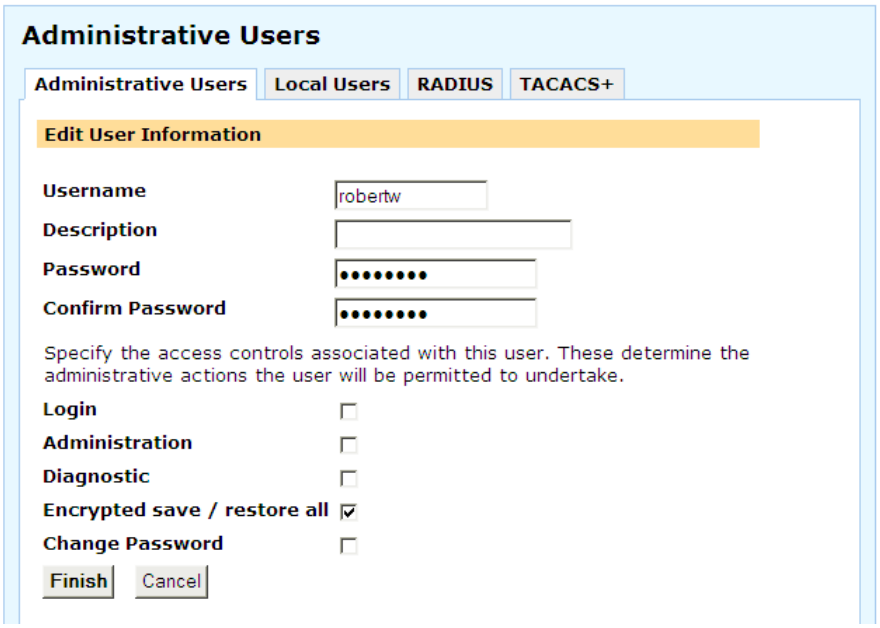
Administrative user accounts on a SG unit allow administrative duties to be spread amongst a number of different people according to their level of competence and trust.

Each administrative user has a password that they use to authenticate when connecting to the web management console, or via telnet or ssh. They also have a number of access controls that modify what they can and cannot do via the web management console

There is one special user, *root*, who has the role of the final administrative user, or super user. The access privileges for this user may not be lowered, and this user may not be deleted or disabled. You may disallow telnet or ssh connections using the root account however.

Select **Users** under the **System** section in the main menu. Existing users are displayed alongside **Delete**, **Edit**, and **Enable/Disable** icons.

Click **New** to add a new user. Enter a **Username** (login name), an optional **Description**, and enter and confirm a **Password**.



You may specify the following access controls for each administrative user.

- The **Login** control provides the user with telnet and ssh access to the command-line administration interface of the SG unit
- The **Administration** control provides the user with the ability to make changes to the SG unit's configuration via the web-based administration interface. This should only be provided to trusted users who are permitted to configure and reconfigure the unit.
- The **Diagnostic** control provides the user with the ability to view restricted diagnostic information via the web-based administration interface. This access control may be given to technical support users so they can attempt to diagnose but not fix any problems which occur.
- The **Encrypted save / restore all** control provides the user to with the ability to save and restore the configuration of the SG unit via the **Save/Restore** page (see the *Save/Restore* section earlier in this chapter). This access control may be given to a technician whom you want to be able to restore the unit to a known good configuration but to whom you do not wish to grant full administration rights.

Warning

*A user with **Encrypted save / restore all** access can conceivably create an encrypted config file with an arbitrary root password that they can restore, thus granting them Administration privileges. Therefore, grant **Encrypted save / restore all** only to users that you trust with **Administration** access.*

- The **Change Password** control provides the user with the ability to change their password.

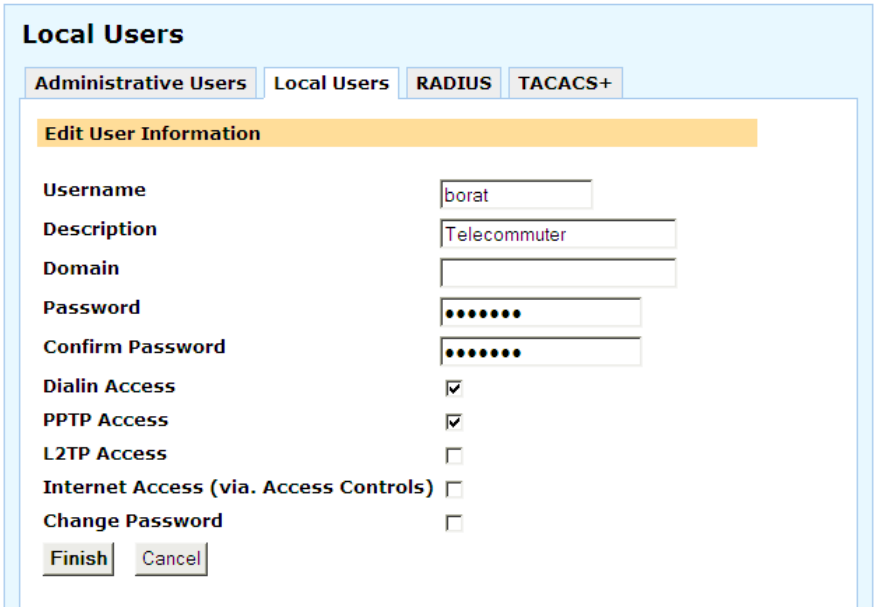
Click **Finish** to apply your changes.

Local Users

Local users accounts are used to grant PPTP, L2TP or dialin access, and access through the access control web proxy (see the *Access Control* section in the chapter entitled *Firewall*).

Select **Users** under the **System** section in the main menu and click the **Local Users** tab. Existing users are displayed alongside **Delete**, **Edit**, and **Enable/Disable** icons.

Click **New** to add a new user.



Enter a **Username** (login name), an optional **Description**, and enter and confirm a **Password**.

For dial-in, PPTP and L2TP users, you may also optionally enter a **Domain** name if your network has a Windows domain server.

You may specify the following access controls for each local user.

- The **Dialin Access** control provides the user with the authority to connect to the SG unit's dialin server.
- The **PPTP Access** control provides the user with the authority to connect to the SG unit's PPTP VPN server (see the *PPTP VPN Server* section of the chapter entitled *VPN*).
- The **L2TP Access** control provides the user with the authority to connect to the SG unit's L2TP server (see the *L2TP VPN Server* section of the chapter entitled *VPN*).
- The **Internet Access (via. Access Controls)** control provides the user with the authority to connect to the Internet, subject to the restrictions defined on the **Access Control** page (see the *Access Control* section of the chapter entitled *Firewall*).
- The **Change Password** control provides the user with the ability to change their password.

Click **Finish** to apply your changes.

RADIUS

The SG unit may be configured to access a central repository of users and passwords on a RADIUS server to authenticate dial-in, PPTP VPN server and L2TP VPN server connections.

Enter the **RADIUS Server** address from which to obtain client authentication information.

Enter the **RADIUS Server Port**. This is usually port 1812, however some older RADIUS servers use port 1645.

Enter and confirm the **RADIUS Secret** used to access the RADIUS server.

Click **Submit** to apply your changes.

TACACS+

The SG unit may be configured to access a central repository of users and passwords on a TACACS+ server to authenticate dial-in, PPTP VPN server and L2TP VPN server connections.

Enter the **TACACS+ Server** address from which to obtain client authentication information.

Enter and confirm the **TACACS+ Secret** used to access the TACACS+ server.

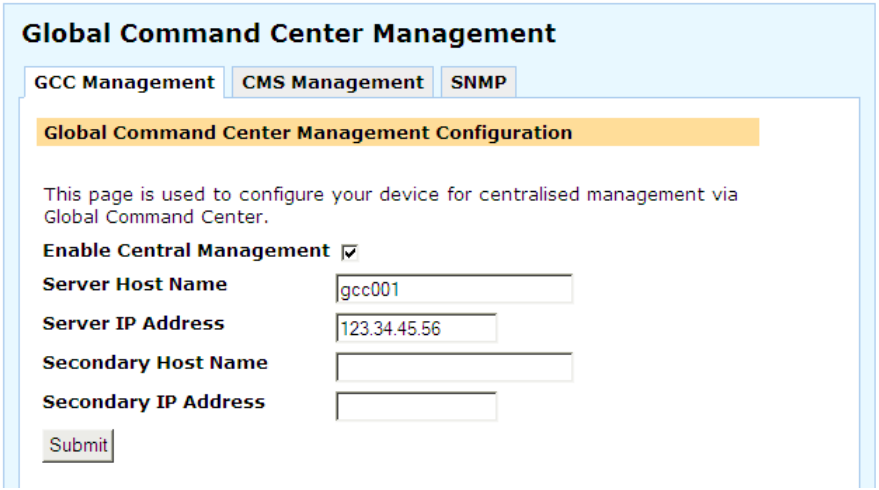
Click **Submit** to apply your changes.

Management

The SG unit may be management remotely using Secure Computing Global Command Center (GCC), Secure Computing Centralized Management Server (CMS) or Simple Network Management Protocol (SNMP).

GCC

To enable remote management by a Secure Computing Global Command Center server, check **Enable Central Management**.



Enter the Global Command Center **Server Host Name**.

Enter the Global Command Center **Server IP Address**. This may be left blank if you want to use DNS name resolution to connect to the Global Command Center server.

If you have a secondary Global Command Center server, enter its name in **Secondary Host Name** so the SG unit's firewall can be updated appropriately.

Enter the IP address of the secondary Global Command Center server in **Secondary IP Address** if applicable.

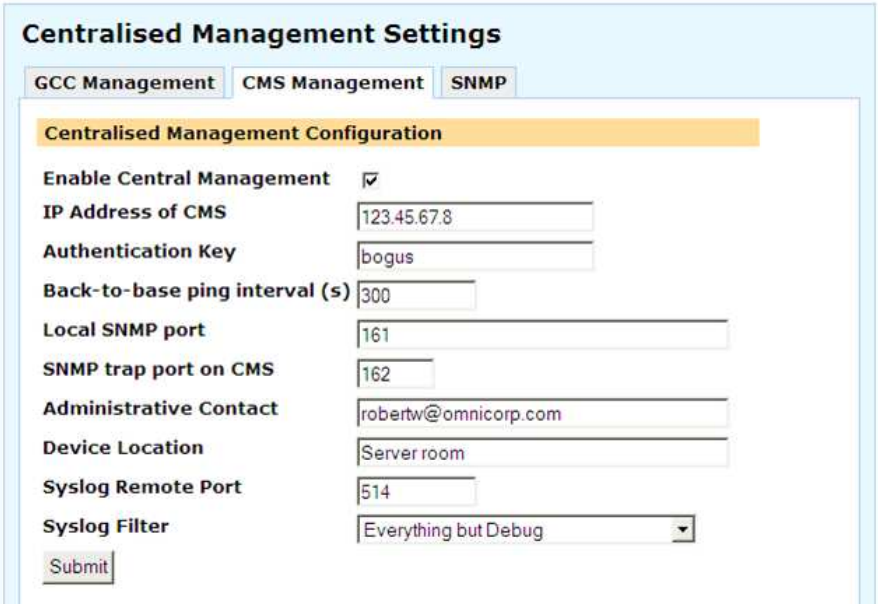
Clicking **Submit** requests a certificate from the Global Command Center server. With the appropriate credentials, you are able to download the appropriate certificates enabling this device to be managed.

Note

Ensure that you have network access and have the Global Command Center server configured appropriately before enabling central management.

CMS

To enable remote management by a Secure Computing Central Management Server, check **Enable Central Management**.



In **IP Address of CMS**, enter the IP address of the host on which Secure Computing CMS is running.

Specify the shared **Authentication Key** with which to authenticates this device against the CMS. This must be the same as the *snmp_community* configuration setting for CMS. It should be something hard to guess.

When configured for centralised management, the device periodically sends a "ping" (SNMP trap) back to the CMS to indicate that it is alive. **Back-to-base ping interval (s)** specifies the interval in seconds between these pings. This must be less than the *max_alive_interval* configuration setting for CMS.

Specify the **Local SNMP Port** on which the management agent listens for requests.

Note

Local SNMP Port *should be changed if you have enabled the SNMP agent under* ***Management*** *->* ***SNMP****.*

Administrative Contact is the SNMP *sysContact* field. Any value may be specified, but a good choice is contact information for the local administrator.

Device Location is the SNMP *sysLocation* field. Any value may be specified, but a good choice is a short description of the physical location of the device.

Enter the **Syslog Remote Port** to which to send syslog messages. This must be the same as the *syslog_port* configuration setting for CMS

Syslog Filter allows setting of a filter for syslog message which are sent to CMS. **Absolutely Everything** sends all messages, including debug messages. This may result in many messages being sent to CMS. **Log Nothing** sends no messages, which can make troubleshooting more difficult. Typically, a setting somewhere between the two is appropriate.

Click **Submit** to apply your changes.

SNMP

To allow external SNMP management software to query this device for management information, check **Enable SNMP Agent**.

Enter the name of a community that is allowed read-only access in **Read-Only Community**. You may optionally include an IP address or network to restrict who is allowed access. You may optionally include an OID to restrict the fields that are accessible.

Enter the name of a community that is allowed read-write access in **Read-Write Community**. You may optionally include an IP address or network to restrict who is allowed access. You may optionally include an OID to restrict the fields that are accessible.

Warning

The community name is equivalent to a password, and is sent in plain text in every SNMP packet. Anyone who knows the community name is able to modify settings on this device. It is highly recommended that you do not allow read-write access, or that you take additional steps to secure the connection.

In **Local SNMP Port**, specify the endpoints on which the SNMP agent accepts requests. An endpoint consists of an optional transport, an optional address, and a port, separated by : (colon) characters. The default transport is UDP, and the default address is any address. For example: **1161**, **tcp:161**, **10.0.0.1:1161**, or **tcp:10.0.0.1:1161**.

Administrative Contact is the SNMP *sysContact* field. Any value may be specified, but a good choice is contact information for the local administrator.

Device Location is the SNMP *sysLocation* field. Any value may be specified, but a good choice is a short description of the physical location of the device.

Click **Submit** to apply your changes.

Diagnostics

Low-level diagnostic information and network tests are provided to assist you in diagnosing network problems.

Diagnostics

To access this diagnostic information, select **Diagnostics** under the **System** section of the main menu. This page displays information including the current firmware version, network settings and the status of Internet and VPN connections.

Network tests

Basic network diagnostic tests (*ping*, *traceroute*) can be accessed by clicking the **Network Tests** tab at the top of the **Diagnostics** page.

Advanced

The following options are intended for network administrators and advanced users *only*.

Warning

Altering the advanced configuration settings may render your SG unit inoperable.

System log

The system log contains debugging information that may be useful in determining whether all services for your SG unit are operating correctly.

Log output is color coded by output type. General information and debug output is black, warnings and notices are blue, and errors are red.

The **Display** pull down menu underneath the log output allows you to filter the log output to display, based on output type.

Appendix B contains for details on interpreting log output and configuring advanced log rules.

Local syslog

By default all messages are recoreded in the System Log. **Filter Level** allows you to control which classes of messages are recorded in the system log.

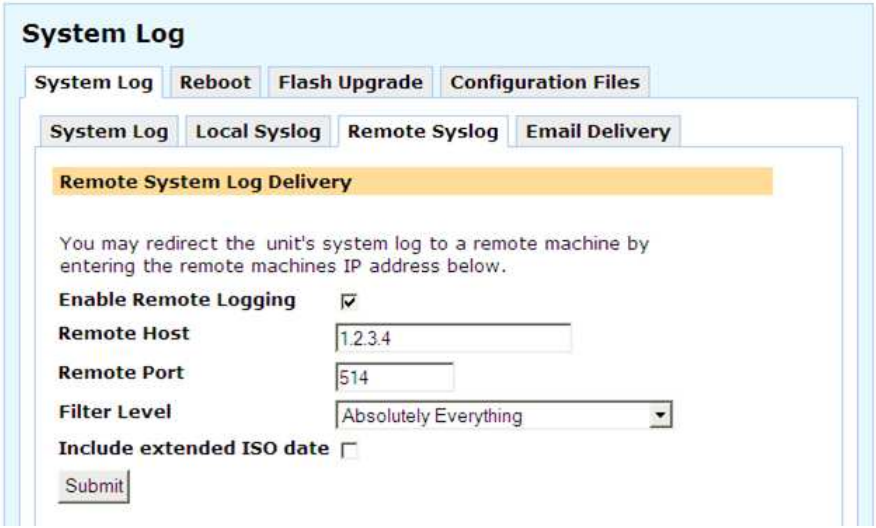
Every message recorded in the System Log includes a basic time stamp. Check **Include extended ISO date** to force a more precise and standardized timestamp to be included with every message.

Click **Submit** to apply your changes.

Remote syslog

System log messages may be sent to a remote syslog server. This allows you to keep system log messages persistently.

Once you have set up a remote syslog server, check **Enable Remote Logging**.



Enter the IP address or DNS hostname for the remote syslog server in **Remote Host**.

Enter the **Remote Port** on which the remote syslog server is listening for syslog messages. Typically, the default is correct.

Set the **Filter Level** to only send syslog messages at this level or above.

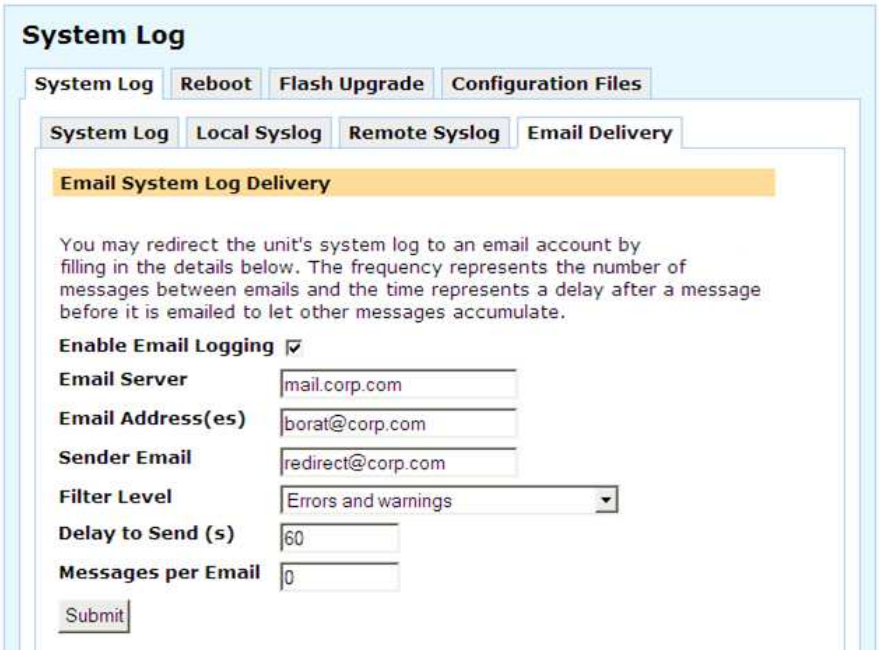
You may also **Include extended ISO date**, which is prepended to syslog messages before being sent.

Click **Submit** to save your changes.

Email delivery

Syslog log messages may be sent to an email account. This allows you to keep system log messages persistently.

Check **Enable Email Logging**.



Enter the address of an **Email Server** (SMTP server) that accepts email for forwarding.

Enter the **Email Address(es)** to which to send the system log messages.

The **Sender Email** address that System Log messages are sent from.

Set the **Filter Level** to only send syslog messages at this level or above.

Specify the number of seconds to wait after recieving a system log message before sending the an email in **Delay to Send (s)**. This allows multiple system log messages to accumulate before sending an email containing them all.

Messages per Email is the maximum number of system log messages that are allowed to accumulate before sending the email. The default setting of 0 means unlimited, and is typically appropriate for all systems but those that experience heavy traffic.

Click **Submit** to apply your changes.

Reboot and Reset

Rebooting does not erase your SG unit's configuration, however network connections such as your Internet connection, VPN tunnels, etc. are terminated and re-established when the device is up and running again.

Warning

Before restoring your SG unit to its default factory settings via the web management console or reset button, it is strongly recommended that you create a back up of your configuration. Refer to the Save/Restore *section earlier in this chapter for details.*

Reboot device

Click **Reboot Now** to have the SG unit to perform a soft reboot. It usually takes around 10 seconds before it is up and running again.

If you have enabled bridging, the SG unit may take up to 30 seconds to reboot. Any shared printers take 30 seconds to become available, during which time print jobs are not accepted.

Erase configuration

To erase your SG unit's configuration and return to the factory default settings, click **Erase Configuration**. This is useful if you want to reconfigure the device form scratch after an upgrade, or want to redeploy the device into a different environment.

Reset button

Another method to clear the SG unit's stored configuration information is by pushing the reset button on the back panel of the SG unit **twice**. A bent paper clip is a suitable tool for performing this procedure.

This is particularly useful should the SG unit become uncontactable, e.g. due to misconfiguration.

Pushing the reset button **twice** clears all stored configuration information, reverts all settings to the factory defaults, and reboots the SG unit.

Note

When the SG unit reboots, it has an IP address of 192.168.0.1, netmask 255.255.255.0.

Disabling the reset button on your SG PCI appliance

For convenience, the SG unit ships with the rear panel Reset button enabled. This allows the SG unit's configuration to be reset to factory defaults.

From a network security standpoint, it may be desirable to disable the Reset switch after initial setup has been performed. This is accomplished by removing the jumper linking *CON2* on the SG unit.

This jumper is labeled *Remove Link to Disable Erase*.

Flash upgrade

Periodically, Secure Computing may release new versions of firmware for your SG unit. If a new version fixes an issue you've been experiencing, or contains a new feature you wish to utilize, contact SG technical support for information on obtaining the latest firmware. You can then load the new firmware with a flash upgrade.

Note

Please read the appendix entitled Firmware Upgrade Practices and Precautions *before attempting a firmware upgrade.*

There are two primary methods available for performing a flash upgrade, *Netflash* and *Flash upgrade via HTTP*. Remote upgrades may also be performed using TFTP if you have a TFTP server at the remote site, see *Flash upgrade via TFTP*.

During the upgrade, the front panel LEDs on the SG unit flash in an in-and-out pattern. The SG unit retains its configuration information with the new firmware.

Warning

If the flash upgrade is interrupted (e.g. power down), the SG unit stops functioning and becomes unusable until its flash is reprogrammed at the factory or a recovery boot is performed. User care is advised.

For instructions on performing a recovery boot, refer to Appendix D, Recovering From a Failed Upgrade*.*

Netflash

The first is to download the *netflash.exe* for the appropriate model and version to which you are upgrading. This is a Windows program that automates the upgrade procedure. Be sure to read the release notes before attempting the upgrade.

Flash upgrade via HTTP

The second is to download the binary image file (*.sgu*). Contact SG technical support for instructions on obtaining this file.

Select **Advanced** from the **System** section of the main menu and click the **Flash Upgrade** tab. Click **Browse** to locate the *.sgu* file on your local PC and click **Upgrade**.

Enter **Extra Parameters** only at the request of Secure Computing technical support staff.

Flash upgrade via TFTP

An alternative method is to install and configure a TFTP server. The majority of Linux distributions include a TFTP server, Windows users can download one from: http://www.snapgear.com/ftp/tools/tftpd32j.zip

Note

Although we recommend it, this program is not supported by Secure Computing.

Download the binary image file (*.sgu*). Contact SG technical support for instructions on obtaining this file. Place this file in the directory your TFTP is serving files from, usually: */tftpboot/*

Establish a telnet or ssh connection to the SG unit. Login and run the command:

```
flash image <TFTP server address> <image.sgu>
```

.. where <*TFTP server address*> is the address of your TFTP server, and <*image.sgu*> is the binary image filename. Your telnet or ssh connection is terminated once the upgrade commences.

Configuration Files

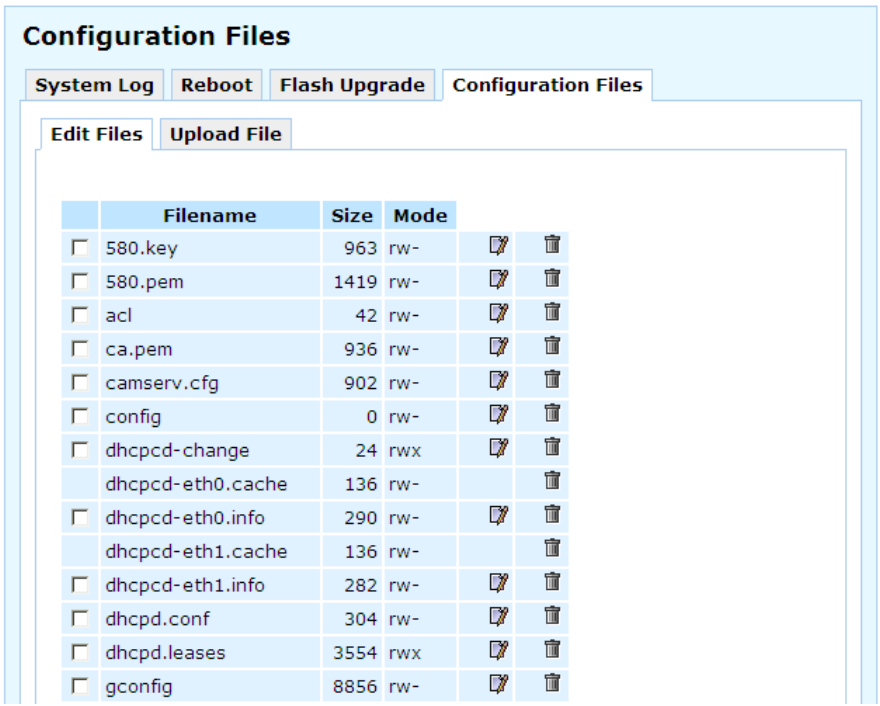
To manually edit, view, or upload new configuration files, select **Advanced** from the **System** section of the main menu and click the **Configuration Files** tab.

Warning

Manually modifying or deleting your SG unit's configuration files may render the unit inoperable until a factory reset has been performed.

Edit files

To modify multiple files at once, check the **Filenames** and click **Modify**. To edit a single file, click its **Edit** icon.



You may also create a new file by clicking **New**.

Upload file

Click **Browse** to locate the file on your local PC that you want to upload. You may upload it to an alternative file name on the SG unit by specifying a **Destination File Name**. Click **Submit** to begin the upload.

Warning

Any existing file with the same name is overwritten

Support

For information on obtaining support for your SG unit, select **Support** from the **System** section of the main menu.

This page provides basic troubleshooting tips, contact details for SG technical support, and links to the SG Knowledge Base (http://www.cyberguard.com/snapgear/knowledgebase.html) as shown in the following figure:

Technical support report

The **Technical Support Report** page is an invaluable resource for the SG technical support team to analyze problems with your SG unit. The information on this page gives the support team important information about any problems you may be experiencing.

Note

*If you experience a fault with your SG unit and have to contact the SG technical support team, **ensure you include the Technical Support Report with your support request**. The Technical Support Report should be generated when the issue is occurring on each of the appliances involved, and attached in plain text format. Otherwise, the Secure Computing technical support staff are unlikely to have enough information to assist you.*

Appendix A – Terminology

This section explains some of the terms that are commonly used in this document.

Term	Meaning
ADSL	Asymmetric Digital Subscriber Line. A technology allowing high-speed data transfer over existing telephone lines. ADSL supports data rates between 1.5 and 9 Mbits/s when receiving data and between 16 and 640 Kbit/s when sending data.
Advanced Encryption Standard (AES)	The Advanced Encryption Standard is a new block cipher standard to replace DES, developed by NIST, the US National Institute of Standards and Technology. AES ciphers use a 128-bit block and 128, 192 or 256-bit keys. The larger block size helps resist birthday attacks while the large key size prevents brute force attacks.
Aggressive Mode	This Phase 1 keying mode automatically exchanges encryption and authentication keys and uses less messages in the exchange when compared to Main mode. Aggressive mode is typically used to allow parties that are configured with a dynamic IP address and a preshared secret to connect or if the SG unit or the remote party is behind a NAT device.
Authentication	Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter. Authentication confirms that data is sent to the intended recipient and assures the recipient that the data originated from the expected sender and has not been altered on route.
Automatic Keying, Internet Key Exchange (IKE)	This type of keying automatically exchanges encryption and authentication keys and replaces them periodically.
Block cipher	A method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time. DES, 3DES and AES are all block ciphers.
BOOTP	Bootstrap Protocol. A protocol that allows a network user to automatically receive an IP address and have an operating system boot without user interaction. BOOTP is the basis for the more advanced DHCP.
CA Certificate	A self-signed certification authority (CA) certificate that identifies a CA. It is called a CA certificate because it is the certificate for the root CA.

Certificates	A digitally signed statement that contains information about an entity and the entity's public key, thus binding these two pieces of information together. A certificate is issued by a trusted organization (or entity) called a Certification Authority (CA) after the CA has verified that the entity is who it says it is.
Certificate Authority	A Certificate Authority is a trusted third party, which certifies public key's to truly belong to their claimed owners. It is a key part of any Public Key Infrastructure, since it allows users to trust that a given public key is the one they wish to use, either to send a private message to its owner or to verify the signature on a message sent by that owner.
Certificate Revocation List	A list of certificates that have been revoked by the CA before they expired. This may be necessary if the private key certificate has been compromised or if the holder of the certificate is to be denied the ability to establish a tunnel to the SG unit.
Data Encryption Standard (DES)	The Data Encryption Standard is a block cipher with 64-bit blocks and a 56-bit key.
Dead Peer Detection	The method of detecting if the remote party has a stale set of keys and if the tunnel requires rekeying. To interoperate with the SG unit, it must conform to the draft draft-ietf-ipsec-dpd-00.txt
DHCP	Dynamic Host Configuration Protocol. A communications protocol that assigns IP addresses to computers when they are connected to the network.
Diffie-Hellman Group or Oakley Group	The groups used as the basis of Diffie-Hellman key exchange in the Oakley protocol, and in IKE.
Diffie-Hellman Key Exchange	A protocol that allows two parties without any initial shared secret to create one in a manner immune to eavesdropping. Once they have done this, they can communicate privately by using that shared secret as a key for a block cipher or as the basis for key exchange.
Distinguished Name	A list of attributes that defines the description of the certificate. These attributes include: country, state, locality, organization, organizational unit and common name.
DNS	Domain Name System that allocates Internet domain names and translates them into IP addresses. A domain name is a meaningful and easy to remember name for an IP address.
DUN	Dial Up Networking.
Encapsulating Security Payload (ESP)	Encapsulated Security Payload is the IPSec protocol which provides encryption and can also provide authentication service.
Encryption	The technique for converting a readable message (plaintext) into apparently random material (ciphertext) which cannot be read if intercepted. The proper decryption key is required to read the message.
Ethernet	A physical layer protocol based upon IEEE standards.

Extranet	A private network that uses the public Internet to securely share business information and operations with suppliers, vendors, partners, customers, or other businesses. Extranets add external parties to a company's intranet.
Failover	A method for detecting that the main Internet connection (usually a broadband connection) has failed and the SG apliance cannot communicate with the Internet. If this occurs, the SG unit automatically moves to a lower speed, secondary Internet connection.
Fall-forward	A method for shutting down the failover connection when the main Internet connection can be re-established.
Firewall	A network gateway device that protects a private network from users on other networks. A firewall is usually installed to allow users on an intranet access to the public Internet without allowing public Internet users access to the intranet.
Gateway	A machine that provides a route (or pathway) to the outside world.
Hashes	A code, calculated based on the contents of a message. This code should have the property that it is extremely difficult to construct a message so that its Hash comes to a specific value.Hashes are useful because they can be attached to a message, and demonstrate that it has not been modified. If a message were to be modified, then its hash would have changed, and would no longer match the original hash value.
Hub	A network device that allows more than one computer to be connected as a LAN, usually using UTP cabling.
IDB	Intruder Detection and Blocking. A feature of your SG unit that detects connection attempts from intruders and can also optionally block all further connection attempts from the intruder's machine.
Internet	A worldwide system of computer networks. A public, cooperative, and self-sustaining network of networks accessible to hundreds of millions of people worldwide. The Internet is technically distinguished because it uses the TCP/IP set of protocols.
Intranet	A private TCP/IP network within an enterprise.
IP Compression	A good encryption algorithm produces ciphertext that is evenly distributed. This makes it difficult to compress. If one wishes to compress the data it must be done prior to encrypting. The IPcomp header provides for this. One of the problems of tunnel mode is that it adds 20 bytes of IP header, plus 28 bytes of ESP overhead to each packet. This can cause large packets to be fragmented. Compressing the packet first may make it small enough to avoid this fragmentation.
IPSec	Internet Protocol Security. IPSec provides interoperable, high quality, cryptographically-based security at the IP layer and offers protection for network communications.
IPSec tunnel	The IPSec connection to securely link two private parties across insecure and public channels.

IPSec with Dynamic DNS	Dynamic DNS can be run on the IPSec endpoints thereby creating an IPSec tunnel using dynamic IP addresses.
IKE	IKE is a profile of ISAKMP that is for use by IPsec. It is often called simply IKE. IKE creates a private, authenticated key management channel. Using that channel, two peers can communicate, arranging for sessions keys to be generated for AH, ESP or IPcomp. The channel is used for the peers to agree on the encryption, authentication and compression algorithms to be used. The traffic to which the policies are applied is also agreed upon.
ISAKMP	ISAKMP is a framework for doing Security Association Key Management. It can, in theory, be used to produce session keys for many different systems, not just IPsec.
Key lifetimes	The length of time before keys are renegotiated.
LAN	Local Area Network.
LED	Light-Emitting Diode.
Local Private Key Certificate & Passphrase	The private part of the public/private key pair of the certificate resides on the SG unit. The passphrase is a key that can be used to lock and unlock the information in the private key certificate.
Local Public Key Certificate	The public part of the public/private key pair of the certificate resides on the SG unit and is used to authenticate against the CA certificate.
MAC address	The hardware address of an Ethernet interface. It is a 48-bit number usually written as a series of 6 hexadecimal octets, e.g. 00:d0:cf:00:5b:da. A SG unit has a MAC address for each Ethernet interface. These are listed on a label on the underneath of the device.
Main Mode	This Phase 1 keying mode automatically exchanges encryption and authentication keys and protects the identities of the parties attempting to establish the tunnel.
Manual Keying	This type of keying requires the encryption and authentication keys to be specified.
Manual Keys	Predetermined encryption and authentication keys used to establish the tunnel.
Masquerade	The process when a gateway on a local network modifies outgoing packets by replacing the source address of the packets with its own IP address. All IP traffic originating from the local network appears to come from the gateway itself and not the machines on the local network.
MD5	Message Digest Algorithm Five is a 128 bit hash. It is one of two message digest algorithms available in IPSec.
NAT	Network Address Translation. The translation of an IP address used on one network to an IP address on another network. Masquerading is one particular form of NAT.
Net mask	The way that computers know which part of a TCP/IP address refers to the network, and which part refers to the host range.

NTP	Network Time Protocol (NTP) used to synchronize clock times in a network of computers.
Oakley Group	See Diffie-Hellman Group or Oakley Group.
PAT	Port Address Translation. The translation of a port number used on one network to a port number on another network.
PEM, DER, PCKS#12 PCKS#07	These are all certificate formats.
Perfect Forward Secrecy	A property of systems such as Diffie-Hellman key exchange which use a long-term key (such as the shared secret in IKE) and generate short-term keys as required. If an attacker who acquires the long-term key provably can neither read previous messages which he may have archived nor read future messages without performing additional successful attacksthen the system has PFS. The attacker needs the short-term keys in order to read the traffic and merely having the long-term key does not allow him to infer those. Of course, it may allow him to conduct another attack (such as man-in-the-middle) which gives him some short-term keys, but he does not automatically get them just by acquiring the long-term key.
Phase 1	Sets up a secure communications channel to establish the encrypted tunnel in IPSec.
Phase 2	Sets up the encrypted tunnel in IPSec.
PPP	Point-to-Point Protocol. A networking protocol for establishing simple links between two peers.
PPPoE	Point to Point Protocol over Ethernet. A protocol for connecting users on an Ethernet to the Internet using a common broadband medium (e.g. single DSL line, wireless device, cable modem, etc).
PPTP	Point to Point Tunneling Protocol. A protocol developed by Microsoft™ that is popular for VPN applications. Although not considered as secure as IPSec, PPP is considered "good enough" technology. Microsoft has addressed many flaws in the original implementation.
Preshared secret	A common secret (passphrase) that is shared between the two parties.
Quick Mode	This Phase 2 keying mode automatically exchanges encryption and authentication keys that actually establishes the encrypted tunnel.
Rekeying	The process of renegotiating a new set of keys for encryption and authentication.
Road warrior	A remote machine with no fixed IP address.
Router	A network device that moves packets of data. A router differs from hubs and switches because it is "intelligent" and can route packets to their final destination.
RSA Digital Signatures	A public/private RSA key pair used for authentication. The SG unit can generate these key pairs. The public keys need to be exchanged between the two parties in order to configure the tunnel.

SHA	Secure Hash Algorithm, a 160 bit hash. It is one of two message digest algorithms available in IPSec.
Security Parameter Index (SPI)	Security Parameter Index, an index used within IPsec to keep connections distinct. Without the SPI, two connections to the same gateway using the same protocol could not be distinguished.
Subnet mask	See "Net mask".
Switch	A network device that is similar to a hub, but much smarter. Although not a full router, a switch partically understands how to route Internet packets. A switch increases LAN efficiency by utilizing bandwidth more effectively.
TCP/IP	Transmission Control Protocol/Internet Protocol. The basic protocol for Internet communication.
TCP/IP address	Fundamental Internet addressing method that uses the form nnn.nnn.nnn.nnn.
TripleDES (3DES)	Using three DES encryptions on a single data block, with at least two different keys, to get higher security than is available from a single DES pass.
UTC	Coordinated Universal Time.
UTP	Unshielded Twisted Pair cabling. A type of Ethernet cable that can operate up to 100Mbits/s. Also known as Category 5 or CAT 5.
VPN	Virtual Private Networking. When two locations commmunicate securely and effectively across a public network (e.g. the Internet). The three key features of VPN technology are privacy (nobody can see what you are communicating), authentication (you know who you are communicating with), and integrity (nobody can tamper with your messages/data).
WAN	Wide Area Network.
WINS	Windows Internet Naming Service that manages the association of workstation names and locations with IP addresses.
x.509 Certificates	An x.509 certificate includes the format of the certificate, the serial number of the certificate, the algorithm used to sign the certificate, the name of the CA that issued the certificate, the name and public key of the entity requesting the certificate, and the CA's signature.x.509 certificates are used to authenticate the remote party against a Certificate Authority's (CA) certificate. The CA certificate must have signed the local certificates that are used for tunnel authentication. Certificates need to be uploaded into the SG unit before a tunnel can be configured to use them (see Certificate Management).

Appendix B – System Log

Access Logging

It is possible to log any traffic that arrives at or traverses the SG unit. The only logging that is enabled by default is to take note of packets that were dropped. While it is possible to specifically log exactly which rule led to such a drop, this is not configured by default. All rules in the default security policy drop packets. They never reject them. That is, the packets are simply ignored, and have no responses at all returned to the sender. It is possible to configure reject rules if so desired.

All traffic logging performed on the SG unit creates entries in the syslog (*/var/log/messages* or external syslog server) of the following format:

```
<Date/Time> klogd: <prefix> IN=<incoming interface>
OUT=<outgoing interface> MAC=<dst/src MAC addresses>
SRC=<source IP> DST=<destination IP> SPT=<source port>
DPT=<destination port> <additional packet info>
```

Where:

<prefix>	if non-empty, hints at cause for log entry
<incoming interface>	empty, or one of eth0, eth1 or similar
<outgoing interface>	as per incoming interface
<dst/src MAC addresses>	MAC addresses associated with the packet
<source IP>	packet claims it came from this IP address
<destination IP>	packet claims it should go to this IP address
<source port>	packet claims it came from this TCP port
<destination port>	packet wants to go to this TCP port

Depending on the type of packet and logging performed some of the fields may not appear.

Commonly used interfaces are:

eth0	the LAN port
eth1	the WAN/Internet port
ppp*X*	e.g. *ppp0* or *ppp1*, a PPP session
ipsec*X*	e.g. *ipsec0*, an IPSec interface

The firewall rules deny all packets arriving from the WAN port by default. There are a few ports open to deal with traffic such as DHCP, VPN services and similar. Any traffic that does not match the exceptions however is dropped.

There are also some specific rules to detect various attacks (smurf, teardrop, etc.).

When outbound traffic (from LAN to WAN) is blocked by custom rules configured in the GUI, the resultant dropped packets are also logged.

The <*prefix*> for all these rules is varied according to their type.

Currently used prefixes for traffic arriving:

Default Deny	Packet didn't match any rule, drop it
Invalid	Invalid packet format detected
Smurf	Smurf attack detected
Spoof	Invalid IP address detected
SynFlood	SynFlood attack detected
Custom	Custom rule dropped outbound packet

A typical *Default Deny:* looks similar to the following:

```
   Mar 27 09:31:19 2003 klogd: Default deny: IN=eth1
OUT=MAC=00:d0:cf:00:ff:01:00:e0:29:65:af:e9:08:00
SRC=140.103.74.181 DST=12.16.16.36 LEN=60 TOS=0x10 PREC=0x00
TTL=64 ID=46341 DF PROTO=TCP SPT=46111 DPT=139 WINDOW=5840
RES=0x00 SYN URGP=0
```

That is, a packet arriving from the WAN (*IN=eth1*) and bound for the SG unit itself (*OUT=<nothing>*) from IP address 140.103.74.181 (*SRC=140.103.74.181*), attempting to go to port 139 (*DPT=139*, Windows file sharing) was dropped.

If the packet is traversing the SG unit to a server on the private network, the outgoing interface is eth0, e.g.:

```
   Mar 27 09:52:59 2003 klogd: IN=eth1 OUT=eth0
SRC=140.103.74.181 DST=10.0.0.2 LEN=60 TOS=0x10 PREC=0x00
TTL=62 ID=51683 DF PROTO=TCP SPT=47044 DPT=22 WINDOW=5840
RES=0x00 SYN URGP=0
```

Packets going from the private network to the public come in eth0, and out eth1, e.g.:

```
   Mar 27 10:02:51 2003 klogd: IN=eth0 OUT=eth1 SRC=10.0.0.2
DST=140.103.74.181 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=62830 DF
PROTO=TCP SPT=46486 DPT=22 WINDOW=5840 RES=0x00 SYN URGP=0
```

Creating Custom Log Rules

Additional log rules can be configured to provide more detail if desired. For example, by analyzing the rules in the **Rules** menu, it is possible to provide additional log messages with configurable prefixes (i.e. other than *Default Deny:*) for some allowed or denied protocols.

Depending on how the *LOG* rules are constructed it may be possible to differentiate between inbound (from WAN to LAN) and outbound (from LAN to WAN) traffic. Similarly, traffic attempting to access services on the SG unit itself can be differentiated from traffic trying to pass through it.

The examples below can be entered on the Command Line Interface (telnet), or into the **Rules** web management console. Rules entered on the CLI are not permanent however, so while it may be useful for some quick testing, it is something to be wary of.

To log permitted inbound access requests to services hosted on the SG unit, the rule should look something like this:

```
iptables -I INPUT -j LOG -p tcp --syn -s <X.X.X.X/XX> -d
<Y.Y.Y.Y/YY> --dport <Z> --log-prefix <prefix>
```

This logs any TCP (*-p tcp*) session initiations (*--syn*) that arrive from the IP address/netmask *X.X.X.X/XX* (*-s ...*) and are going to *Y.Y.Y.Y/YY*, destination port Z (*--dport*).

For example, to log all inbound access requests from anywhere on the Internet (0.0.0.0/0) to the PPTP service (port 1723) on the SG unit (IP address 1.2.3.4):

```
iptables -I INPUT -j LOG -p tcp --syn -s 0.0.0.0/0 -d 1.2.3.4 -
-dport 1723 --log-prefix "Internet PPTP access: "
```

To find the resultant log entry in the logs, simply search for the prefix, in this instance *"Internet PPTP access: "*.

If for example site 192.0.1.2 attempted to access the SG unit's PPTP port, the resultant log message would look something like this:

```
<12> Jan 24 17:19:17 2000 klogd: Internet PPTP access: IN=eth0
OUT= MAC=00:d0:cf:00:07:03:00:50:bf:20:66:4d:08:00 SRC=
DST=1.2.3.4 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=43470 DF
PROTO=TCP SPT=4508 DPT=1723 WINDOW=64240 RES=0x00 SYN URGP=0
```

Note how *OUT* is set to nothing. This indicates that the packet was attempting to reach a service on the SG unit, rather than attempting to pass through it.

A very similar scenario occurs for logging access requests that are attempting to pass through the SG unit. It merely requires replacing the *INPUT* keyword with *FORWARD*.

Thus, to log permitted inbound requests to services hosted on a server behind the SG unit, or outbound requests to services on a public network server, use:

```
iptables -I FORWARD -j LOG -p tcp --syn -s <X.X.X.X/XX> -d
<Y.Y.Y.Y/YY> --dport <Z> --log-prefix <prefix>
```

For example, to log all inbound requests from the IP address 5.6.7.8 to the mail server (port 25) on the machine *flubber* on the LAN with address 192.168.1.1:

```
iptables -I FORWARD -j LOG -p tcp --syn -s 5.6.7.8/32 -d
192.168.1.1 --dport 25 --log-prefix "Mail for flubber: "
```

This results in log output similar to:

```
<12> Jan 24 18:17:19 2000 klogd: Mail for flubber: IN=eth1
OUT=eth0 SRC=5.6.7.8 DST=192.168.1.1 LEN=48 TOS=0x00 PREC=0x00
TTL=126 ID=45507 DF PROTO=TCP SPT=4088 DPT=25 WINDOW=64240
RES=0x00 SYN URGP=0
```

Note how the *OUT* value has now changed to show which interface the access attempt used to reach the internal host. As this request arrived on eth1 and was destined for eth0, we can determine that it was an *inbound* request, since eth0 is the LAN port, and eth1 is usually the WAN port.

An *outbound* request would have *IN=eth0* and *OUT=eth1*.

It is possible to use the *-i* and *-o* arguments to specify the interface that are to be considered for *IN* and *OUT* respectively. When the *!* argument is used before the interface name, the sense is inverted. A name ending in a + matches any interface that begins with the name. e.g.

```
iptables -I FORWARD -j LOG -i eth0 -p tcp ...
```

This rule logs outbound from the LAN (eth0) only. We could limit that further by specifying which interface it is outbound to, by using the *-o* option.

```
iptables -I FORWARD -j LOG -i eth0 -o eth1 -p tcp ...
```

This logs LAN traffic destined for the WAN, but won't log LAN traffic destined for a PPP or perhaps IPSec link.

Similarly, we could construct a rule that looks at all inbound/outbound traffic, but excludes VPN traffic, thus:

```
iptables -I FORWARD -j LOG -i eth+ -o eth+ -p tcp ...
```

If we just wanted to look at traffic that went out to the IPSec world, we could use:

```
iptables -I FORWARD -j LOG -o ipsec+
```

Clearly there are many more combinations possible.

It is therefore possible to write rules that log inbound and outbound traffic, or to construct several rules that differentiate between the two.

Rate Limiting

iptables has the facility for rate-limiting the log messages that are generated, in order to avoid denial of service issues arising out of logging these access attempts. To achieve this, use the following option:

`--limit` ***`rate`***

rate is the maximum average matching rate, specified as a number with an optional */second*, */minute*, */hour*, or */day* suffix. The default is *3/hour*.

`--limit-burst` ***`number`***

number is the maximum initial number of packets to match. This number gets recharged by one every time the limit specified above is not reached, up to this number. The default is *5*.

iptables has many more options. Perform a web search for *manpage iptables* to find the relevant documentation.

The *LOG* rules configured by default (e.g. *Default Deny:*) are all limited to:

```
--limit 3/hour --limit-burst 5
```

Administrative Access Logging

When a user tries to log onto the web management console, one of the following log messages appears:

```
Jan 30 03:00:18 2000 boa: Authentication successful for root
from 10.0.0.2
```

```
Jan 30 03:00:14 2000 boa: Authentication attempt failed for
root from 10.0.0.2
```

This message shows the date/time, whether the authentication succeeded or failed, the user attempting authentication (in this case *root*) and the IP address from which the attempt was made.

Telnet (Command Line Interface) login attempts appear as:

```
Jan 30 03:18:37 2000 login: Authentication attempt failed for
root from 10.0.0.2
```

```
Jan 30 03:18:40 2000 login: Authentication successful for root
from 10.0.0.2
```

Once again, showing the same information as a web login attempt.

Boot Log Messages

The SG unit's startup boot time messages are identified by log messages similar to the following:

```
klogd: Linux version 2.4.20-uc0 (jamma@daniel) (gcc version
3.0.4) #4 Mon Feb 3 15:17:50 EST 2003
```

This also shows the version of the operating system (linux), and the build date and time.

Appendix C – Firmware Upgrade Practices and Precautions

Prior performing any firmware upgrade, it is important that you save a back up of your existing configuration (see the *Save/Restore* section in the chapter entitled *System*) to a local file.

While we make every effort to ensure your existing configuration continues working after minor and patch revision upgrades, sometimes compatibility problems may arise.

For major upgrades, existing configuration is not maintained. A factory reset must be performed and the SG unit reconfigured from scratch.

Note

SG firmware revision numbers have the form a.b.c*, where* a *is the major revision number,* b *is the minor revision number, and* c *is the patch revision number.*

An upgrade where the major revision number is incremented is considered a major upgrade, e.g. 2.1.5 -> 3.0.0. An upgrade where the minor revision number is incremented is considered a minor upgrade, e.g. 3.0.2 -> 3.1.0. An upgrade where the patch revision is incremented is considered a patch upgrade, e.g. 3.0.0 -> 3.0.1.

Warning

If the flash upgrade is interrupted (e.g. power down), the SG unit stops functioning and becomes unusable until its flash is reprogrammed at the factory or a recovery boot is performed. User care is advised.

After the upgrade has completed successfully and the SG unit is back up and running with the new firmware, run through a few tests.

Ensure that Internet connectivity and any VPN connections can be established and pass traffic, and that any configured services such as **DHCP Server**, **Access Control** or **Packet Filtering** are functioning as expected.

If you encounter any problems, reset the device to its factory default settings and reconfigure. You may wish to use your backed up old configuration as a guide in this process, but *do not* restore it directly.

If you are upgrading a device that you do not normally have physical access to, e.g. at a remote or client's site, we strongly recommend that following the upgrade, you reset the device to its factory default configuration and reconfigure as a matter of course.

Note

To restore factory default settings, press the black Reset / Erase button on the rear panel twice.

Appendix D – Recovering From a Failed Upgrade

If the *Heart beat* (or *H/B)* LED is not flashing 20 – 30 seconds after power is supplied, the SG unit is unable to boot correctly. This is usually because the firmware inside the SG unit has been written incorrectly or incompletely, or in rare cases it may have become corrupted.

In this situation, a *recovery boot* reprograms the SG to bring it back to a usable state. This can be done using the Netflash executable if you are running Windows, otherwise you have to set up a BOOTP (DHCP) server.

Both procedures are outlined below.

Note

A Netflash that contains the firmware that shipped with your unit is located in the \firmware *directory on the SG CD. A Netflash containing the latest firmware for your SG unit can be obtained from SG customer support.*

Always attempt a recovery boot before requesting an RMA from customer support.

Recovery using Netflash

The following details the steps required to perform a recovery boot using the Netflash program on a Windows PC.

Attach the SG unit's LAN port or switch directly to your PC using a crossover cable.

Note

If you are using an older LITE(2)/LITE(2)+, you may have to attach the unit's WAN port directly to your PC using a crossover cable for the first stage of the recovery procedure. The Netflash program prompts you to switch the cable to the LAN port/switch using a straight through for the second stage of the recovery procedure.

Log in to your PC with administrator privileges (2000/XP/NT4 only).

Ensure there are no DHCP server programs or services (**Start** -> **Run** -> **Open:** *services.msc*) running on your PC.

Disable the inbuilt Windows firewall (**Control Panel** -> **Windows Firewall**), and any third party firewall or antivirus software.

Hold in the **Reset**/**Erase** button while applying power, keep it held in for 3 seconds.

Double click on Netflash to launch it.

Click **Recover** and select **Network Recovery**.

Click **Recover Device**.

Enter an address in the same network range as your PC and click OK

Note

If the recovery procedure fails at or after Assigning IP address.., *but the* Heart Beat/H/B *light is flashing, the unit may have become uncontactable due to bad configuration. If this is the case, hit the* Reset/Erase *button twice within 2 seconds to restore factory default configuration, power off the unit and restart the recovery procedure from the beginning.*

If prompted, select your SG unit from the list displayed.

Enter your SG unit's password and click OK.

If prompted, enter your SG unit's web administration port.

Wait for the recovery procedure to complete and the SG unit to finish reprogramming.

Note

It takes a few minutes for your SG to finish reprogramming. After it has finished it reboots automatically with its old configuration intact. If it is uncontactable after rebooting, hit the Reset/Erase button twice within 2 seconds to restore factory default configuration, then follow the instructions in the chapter entitled Getting Started *to begin reconfiguration of your unit.*

Recovery using a BOOTP server

The following is a brief guide to performing a recovery boot when you are unable to access either Netflash or a Windows PC on which to run it. More comprehensive instructions are not given, as they vary depending on your operating system and server software packages.

The recovery procedure involves network booting the unit using a BOOTP server with access to a SG firmware image file, then upgrading the network as per a normal flash upgrade to reprogram its flash to a usable state.

Note

To perform the recovery boot, you must have a firmware image for your SG unit. The firmware that shipped with your unit is located in the \firmware *directory on the SG CD. The latest firmware for your SG unit can be obtained from SG customer support*

Firmware files have the format Model_Version_Date.sgu *or* Model_Version_Date_*.sgu*.*

Log in to your PC with sufficient permissions to edit the server configuration files, and stop and start the servers.

Place the firmware file in your BOOTP server's path, e.g.: */tftpboot/*

Edit your BOOTP server configuration to contain an entry for the SG unit. Specify the firmware file as the file to boot, e.g.:

```
filename "SG300_v2.1.3_20041213.sgu";
```

(Re)start the BOOTP server.

Attach the SG unit's LAN port or switch directly to your PC using a crossover cable.

Note

If you are using an older LITE(2)/LITE(2)+, you may have to attach the unit's WAN port directly to your PC using a crossover cable for the first stage of the recovery procedure

Accordingly, your BOOTP server requires an entry specifying the SG unit's WAN port MAC address.

Hold in the **Reset**/**Erase** button while applying power, keep it held in for 3 seconds.

After 20 – 30 seconds, the SG unit loads the file from the DHCP/BOOTP server and the *Heart Beat*/*H/B* light begins flashing.

Browse or telnet/ssh to your SG unit and perform a flash upgrade as per usual to reprogram its flash.

Note

If the SG unit is uncontactable, but the Heart Beat/H/B *light is flashing, it may be due to bad configuration. If this is the case, hit the* Reset/Erase *button twice within 2 seconds to restore factory default configuration, and perform the network boot again.*